CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA

SÉRGIO HENRIQUE OLIVEIRA PEREIRA

UMA PROPOSTA DE CLASSIFICAÇÃO PARA RISCOS OPERACIONAIS E SUA DISPOSIÇÃO EM UMA ESTRUTURA TAXONÔMICA PARA EMPRESAS DO MERCADO SEGURADOR BRASILEIRO SOB A VISÃO DA SEGURANÇA DA INFORMAÇÃO

São Paulo

Junho – 2011

SÉRGIO HENRIQUE OLIVEIRA PEREIRA

UMA PROPOSTA DE CLASSIFICAÇÃO PARA RISCOS OPERACIONAIS E SUA DISPOSIÇÃO EM UMA ESTRUTURA TAXONÔMICA PARA EMPRESAS DO MERCADO SEGURADOR BRASILEIRO SOB A VISÃO DA SEGURANÇA DA INFORMAÇÃO

Dissertação apresentada como exigência parcial para obtenção do Título de Mestre em Tecnologia no Centro Estadual de Educação Tecnológica Paula Souza, no Programa de Mestrado em Tecnologia: Gestão e Desenvolvimento de Tecnologias da Informação Aplicadas sob orientação do Prof. Dr. Napoleão Verardi Galegale.

São Paulo
Junho – 2011

SÉRGIO HENRIQUE OLIVEIRA PEREIRA

UMA PROPOSTA DE CLASSIFICAÇÃO PARA RISCOS OPERACIONAIS E SUA DISPOSIÇÃO EM UMA ESTRUTURA TAXONÔMICA PARA EMPRESAS DO MERCADO SEGURADOR BRASILEIRO SOB A VISÃO DA SEGURANÇA DA INFORMAÇÃO

_____

PROF. DR. NAPOLEÃO VERARDI GALEGALE

_____

PROF. DR. ARISTIDES NOVELLI FILHO

_____

PROF. DR. ANTONIO DE LOUREIRO GIL

São Paulo, 13 de junho de 2011.

DEDICATÓRIA

A minha amada esposa **Elizete** e meus amados filhos **Henrique**, **Sophia** e **Nicole**, razão do meu viver.

AGRADECIMENTOS

Agradeço em primeiro lugar a **Deus**, por me dar sabedoria e acima de tudo condições e forças para a realização desse curso.

Agradeço à minha esposa **Elizete**, que sempre esteve do meu lado apoiando e incentivado o andamento de todo o trabalho.

Ao Professor Dr. **Napoleão** Verardi Galegale, pela paciência e dedicação na orientação dessa dissertação.

Sou grato também aos meus **amigos** de curso, pelo apoio e bom convívio ao longo destes dois anos.

Agradeço à **Pamcary** e toda sua **equipe** que proporcionou a realização do curso e que mostrou seu apoio sempre que necessário.

Aos meus amigos **Valdeci** Francisco Pereira Coelho e **Marco** Antonio Pereira Fenoglio que me deram suporte sempre que necessário.

Por fim, agradeço a todas as **pessoas** que direta ou indiretamente tornaram possível a elaboração deste trabalho.

"Se deixamos para última hora, não significa que somos incompetentes... pelo contrário... somos audaciosos.”

Sergio Henrique Oliveira Pereira

RESUMO

PEREIRA, S.H.O.. **Uma Proposta de Classificação para Riscos Operacionais e sua Disposição em uma Estrutura Taxonômica para Empresas do Mercado Segurador Brasileiro Sob a Visão da Segurança da Informação**. 2011. XX f. Dissertação (Mestrado em Tecnologia) - Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2011.

Esta pesquisa tem como principal propósito a criação de uma taxonomia de riscos operacionais, do mercado segurador brasileiro, que estejam relacionados com Segurança da Informação. Essa taxonomia, e consequentemente seus relacionamentos, é peça fundamental para o alinhamento dos conceitos de risco operacional no setor. A informação tem se tornado um ativo de valor incalculável, intangível, para as corporações e o mercado. A necessidade e importância de se ter a informação de forma organizada e tratada a fim de apoiar os interesses do negócio tem sido mostrada constantemente pelo crescente número de incidentes ao redor do mundo. Para o mercado segurador brasileiro não é diferente e Segurança da Informação, mais do que nunca, torna-se relevante para que a informação tenha fluidez através dos recursos disponíveis em TI. Reunindo as técnicas de classificação e disponibilização da informação através da taxonomia e Segurança da Informação, a pesquisa entrega uma proposta para apoiar o setor em questão.

Palavra-chave: Taxonomia; Segurança da Informação; Risco Operacional; Mercado Segurador; Risco.

ABSTRACT

PEREIRA, S.H.O.. **Uma Proposta de Classificação para Riscos Operacionais e sua Disposição em uma Estrutura Taxonômica para Empresas do Mercado Segurador Brasileiro Sob a Visão da Segurança da Informação**. 2011. XX f. Dissertação (Mestrado em Tecnologia) - Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2011.

The main purpose of this research is a creation, for the Brazilian insurance market, an operational risk taxonomy, which is related to Information Security. This taxonomy, and consequently their relationships, is the key to the alignment of the concepts of operational risk in the sector. Information has become an asset of incalculable value, intangible, for corporations and the market. The necessity and importance of having the information in an organized manner and treated in order to support the interests of business has been shown by the constantly increasing number of incidents around the world. For the Brazilian insurance market could not be different and Information Security, more than ever, becomes relevant to contribute in a way that information can flow through the available IT resources. Combining the techniques of classification and how to make information available through the taxonomy and Information Security, the research delivers a proposal to support the sector in question.

Keywords: Taxonomy; Information Security; Operational Risk; Insurance Market; Risk

LISTA DE FIGURAS

SUMÁRIO

1. INTRODUÇÃO

De forma geral observamos o crescimento e valorização da informação para as corporações. Já reconhecida como um ativo intangível, para estas corporações surge um grande desafio de tornar seus sistemas de informação, recursos eficientes e capazes de prover insumo à tomada de decisões alinhadas à estratégia corporativa. Apesar da importância evidente da informação, da forma como organizá-la e principalmente protegê-la, ainda são pequenas as iniciativas que buscam de forma ideal alcançar o que realmente é necessário para torná-la recurso-chave para o corpo de executivos das corporações. Desta forma, aqueles que geram informação dentro das corporações se destacam em relação a aqueles que a utilizam, isso se dá em função da capacidade desses geradores de informação organizá-la e transformá-la em ações eficazes (DRUCKER, 1999). Em outras palavras, é evidenciada a necessidade e importância da informação de forma organizada a serviço dos interesses da gestão estratégica e governança corporativa.

No contexto da era digital é fundamental que os sistemas de informação sejam completos e que toda a informação seja tratada de acordo com a necessidade do negócio. Comumente as questões de Segurança da Informação não são abordadas em níveis executivos das corporações gerando um distanciamento entre a informação e a tomada de decisão.

Para um mercado que, mesmo diante de um cenário de saída de crise mundial, cresceu 14,91% em 2009, segundo a Superintendência de Seguros Privados – SUSEP, não poderia ser diferente. Com faturamento em 2009 de mais de R$ 100 bilhões, incluindo mercados de seguros, previdência e capitalização, o mercado segurador brasileiro mostra sua força e participação efetiva na economia nacional com mais de 3,5% do PIB (CNSEG, 2010).

Segurança da Informação, mais do que nunca, torna-se relevante se considerarmos os grandes investimentos realizados pelas organizações com o intuito de garantir a fluidez da informação através dos recursos disponíveis em TI. Assim, um mapeamento adequado dos riscos inerentes ao negócio, uma padronização conceitual dos mesmos e as possíveis medidas de mitigação dos mesmos, fazem-se necessários para que Segurança da Informação seja incorporada no organismo corporativo de forma que todo investimento em segurança computacional agregue valor de forma eficiente e eficaz ao negócio.

Tradicionalmente, a taxonomia teve por função a classificação das espécies em botânica e zoologia. Agora, aplicada a sistemas de informação, esta ciência terá como principal objetivo a padronização conceitual para riscos do mercado segurador brasileiro. Atualmente, são estruturas classificatórias que têm por finalidade servir de instrumento para a organização e recuperação de informação nas corporações. São esses mapas conceituais que nos ajudarão nessa padronização. O desenvolvimento de taxonomias para o negócio corporativo é considerado um dos pilares da gestão da informação e do conhecimento (BAILEY, 1994).

Ao longo do tempo padrões e normas foram adotados pelo mercado com o intuito de endereçar adequadamente o gerenciamento de riscos dentro da corporação. Esta normatização é mais uma evidência da crescente importância da Segurança da Informação. Documentos de relevância são as normas da família ISO (*The International Organization for Standardization*)/IEC (*The International Electrotechnical Commission*) 27000, *CobiT* (*Control Objectives for Information and Related Technology*) e *ITIL* (*Information Technology Infrastructure Library*) onde o assunto ganha atenção especial e com foco no negócio com sessões específicas para o tratamento de riscos e da Segurança da Informação. Outras regulamentações utilizadas de forma global como a lei americana promulgada em 30 de Junho de 2002 pelos Senadores Paul Sarbanes e Michael Oxley , Sarbanes-Oxley - SOX e o Acordo de Basiléia, oficialmente denominado *International Convergence of Capital Measurement and Capital Standards* e revisado em 2004 (Basiléia II), tem exigido das corporações maior rigor no tratamento da informação de forma geral, exigindo assim que a segurança da informação seja aplicada com maior seriedade e voltada para o negócio.

1.1. Justificativa da pesquisa

Com o notável desempenho do mercado segurador e sua influência na economia do país, são crescentes as preocupações que acerca sua operação. Novas regulamentações, e leis criam novas exigências para que as empresas do mercado segurador implementem novos controles, na tentativa de diminuição de fraudes e/ou ineficiência em seus processos. Apesar das normativas definirem fortemente exigência de novos controles na operação da gestão de riscos, o nível de

detalhamento e classificação de riscos operacionais ainda se encontra incipiente. Dessa forma, alguns dos problemas da operação de gestão de riscos das empresas do mercado segurador brasileiro são abordados nesta pesquisa:

1) Na rotina de gestão de risco geralmente não há, de forma padronizada, uma classificação de riscos com a visão da Segurança da Informação.
2) Necessidade de um modelo de risco operacional de forma a facilitar os processos de gestão de risco.
3) Segregação da informação no mercado segurador referente a classificação de riscos. Não há uma classificação única para riscos dentro do mercado segurador brasileiro.

1.2. Hipótese de trabalho

Para que haja a disseminação dos riscos operacionais do mercado segurador brasileiro e sua padronização (classificação) entre as empresas desse mercado, é necessária a utilização de modelo para a representação comum a todos os usuários daquela informação.

Tais modelos de representação da informação e do conhecimento possibilitam “[...] a elaboração de linguagens documentárias verbais e notacionais, visando à recuperação de informações e organização dos conteúdos informacionais de documentos. No âmbito da terminologia, esses mesmos mecanismos permitem a sistematização dos conceitos e, consequentemente, a elaboração de definições consistentes” (CAMPOS, 2004).

Desta forma, a solução do problema formulado é oferecida através da hipótese da padronização da classificação para riscos operacionais, dispostos em uma estrutura taxonômica, para empresas do mercado segurador brasileiro.

1.3. Objetivos da pesquisa

A pesquisa tem como principal objetivo a proposta de classificação para riscos operacionais e sua disposição em uma estrutura taxonômica para empresas do mercado segurador brasileiro sob a visão da Segurança da Informação. Além dos seguintes objetivos específicos:

- Contribuir para o detalhamento da classificação de riscos para o mercado segurador conforme disposto no item 2.2 desta pesquisa.
- Contribuir para o melhor entendimento dos conceitos relacionados a taxonomia e também seus diversos tipos, conforme no item 2.3 desta pesquisa.
- Analisar a aderência do modelo proposto em empresas do mercado segurador.

1.4. Metodologia de pesquisa

Segundo Gil (GIL, 2002) a pesquisa pode ser definida como o procedimento racional e sistemático que tem como objetivo proporcionar respostas aos problemas que são propostos. Através de métodos, técnicas e outros procedimentos científicos e do próprio conhecimento, desenvolvemos a pesquisa que ao longo de um processo com inúmeras fases que vão desde a identificação do problema até a própria apresentação dos resultados (GIL, 2002).

Para que os objetivos desta pesquisa fossem alcançados dois métodos foram utilizados: o tipológico onde o pesquisador cria modelos idealizados, caracterizando-os através da investigação da realidade e o monográfico ou estudo de caso onde devido ao aprofundamento do estudo busca-se a generalização do objeto de estudo. Assim, estudos sobre riscos para o mercado segurador e construção de estruturas taxonômicas foram desenvolvidos com o intuito de modelar uma proposta de classificação para riscos operacionais e sua estrutura taxonômica para empresas do mercado segurador brasileiro, aplicando-se ao estudo de caso em empresa do mesmo mercado.

A solução para o problema formulado no item 1.1 é respondida com a hipótese de padronização da classificação para riscos operacionais, dispostos em uma estrutura

taxonômica, para empresas do mercado segurador brasileiro. Os demais elementos requeridos por uma pesquisa, segundo Gil (GIL, 2002), são contemplados através da utilização do protocolo do estudo de caso, que possui regras específicas para, entre outras coisas, a coleta de dados.

1.5. Estrutura do trabalho

A estrutura do trabalho está divida em capítulos e/ou seções como segue: introdução, fundamentação teórica, Taxonomia proposta para riscos operacionais relacionados à Segurança da Informação para o mercado segurador, taxonomia proposta para riscos operacionais relacionados à Segurança da Informação para o mercado segurador, estudo de caso e por fim a conclusão da pesquisa.

No primeiro capítulo, a introdução, fornece uma visão geral a respeito do tema e os componentes a seu redor que levaram às questões de pesquisa. No intuito de buscar as respostas para esses questionamentos, foram propostos o objetivo principal e quatro objetivos específicos.

O segundo capítulo mostra todo o referencial teórico, abordando o conteúdo necessário para o entendimento de temas como mercado segurador, risco, taxonomia, segurança da informação, governança e alinhamento estratégico.

O terceiro capítulo é reservado para a apresentação da proposta de classificação taxonômica para riscos operacionais e sua estrutura taxonômica para empresas do mercado segurador brasileiro sob a visão da Segurança da Informação. O modelo terá sua aderência verificada através de estudo de caso conforme já descrito.

No quarto capítulo detalha-se o estudo de caso propriamente dito, seguindo todas as diretrizes do protocolo do estudo de caso passando por visão geral, procedimentos de campo, questões e relatório (YIN, 2001).

Finalmente, no quinto capítulo, apresentamos as conclusões da pesquisa e as perspectivas para trabalhos futuros.

2. FUNDAMENTAÇÃO TEÓRICA

Na seção anterior foram apresentadas a introdução, justificativa da pesquisa (apresentação do problema de pesquisa), hipótese de trabalho, os objetivos, a metodologia de pesquisa e a estrutura para essa dissertação. Nesta seção será discutido o referencial teórico-empírico adotado para embasar a pesquisa realizada.

2.1. MERCADO SEGURADOR BRASILEIRO

A indústria de seguros no Brasil teve sua existência iniciada já no século XVI, através da criação de formas de mutualismo ligadas à assistência, pelo o Padre José de Anchieta. A regulamentação mais antiga de que se tem conhecimento foram as promulgadas 'Regulamentações da Casa de Seguros de Lisboa' com data de 11 de Agosto de 1791, e válidas até a proclamação da república em 1822 (FENASEG, 2011).

Podemos dizer que ao longo dessa história multissecular, o seguro no Brasil teve suas instituições, empresas de seguro, tipo de produtos e o perfil dos profissionais atuantes na área, foram definidos pela própria sociedade. A intervenção por parte do órgão fiscalizador surge juntamente com a complexidade e diversidade dos negócios do mercado. Tal intervenção foi concretizada através de normas de forma a assegurar o cumprimento das coberturas contratadas pelos segurados.

O Sistema Nacional de Seguros Privados foi instituído pelo governo em 1966, pelo decreto-lei 73, com a criação da Superintendência de Seguros Privados – SUSEP que tem como objetivo principal controlar e fiscalizar a constituição e funcionamento das sociedades seguradoras e entidades abertas de previdência privada. Historicamente as empresas do mercado segurador tinham uma articulação pequena e excessivamente cautelosa. A mudança desse comportamento foi marcada pela Carta de Brasília, primeira manifestação conjunta e consensual das empresas de seguro, que claramente definia três princípios: compromisso com a economia de mercado e a livre competição, responsabilidade econômica e social do setor de seguros diante dos agentes produtivos e da população brasileira, e opção pela modernidade que se baseia na experiência do próprio mercado. A ênfase da carta foi dada a desregulamentação do setor, a participação das empresas do mercado segurador junto ao governo nos assuntos e operacionalização da previdência no

Brasil, maior liberdade na operação do seguro-saúde entre outras (FENASEG, 2011). Surge então, através da ação conjunta entre Instituto de Resseguros do Brasil, SUSEP e Secretaria de Política Econômica, um Plano Diretor do Sistema de Seguros, Capitalização e Previdência Complementar. O documento apoiava as reivindicações das empresas do mercado segurador, reafirmando a importância da desregulamentação do setor, apresentando propostas de modernização da atividade seguradora no país, destacando-se: política de liberação de tarifas, abertura do setor ao capital estrangeiro, regulamentação de novas modalidades de seguro, redefinição do papel do correto, etc.

A história do seguro no Brasil é marcada por duas importantes ações de natureza legal e administrativa em 1996: a liberação da entrada de empresas estrangeiras no mercado e a quebra do monopólio ressegurador do IRB. Seguindo então a tendência mundial de globalização dos mercados, processo que quebra barreiras geográficas, o país se mostra tentador para os capitais estrangeiros que somente em 1998 recebeu mais de U$28,7 bilhões em investimentos estrangeiros diretos. A abertura do mercado segurador ao capital externo já era visível em 1996 e 1997 e com as fusões de seguradoras brasileiras e estrangeiras, a participação dessas empresas no total de prêmios arrecadados no Brasil tem um aumento considerável, em 1994 representava apenas 4,16%, subindo para 21,12% no primeiro semestre de 1998 (FENASEG, 2011).

Atualmente o Sistema Nacional de Seguros Privados é integrado pelo Conselho Nacional de Seguros Privados – CNSP, Superintendência de Seguros Privados – SUSEP e sociedades autorizadas a operar em seguros privados e capitalização, entidades abertas de previdência complementar e corretores de seguros habilitados. Seu organograma é mostrado na Figura 1 e sua representação institucional na Figura 2, ambas abaixo.

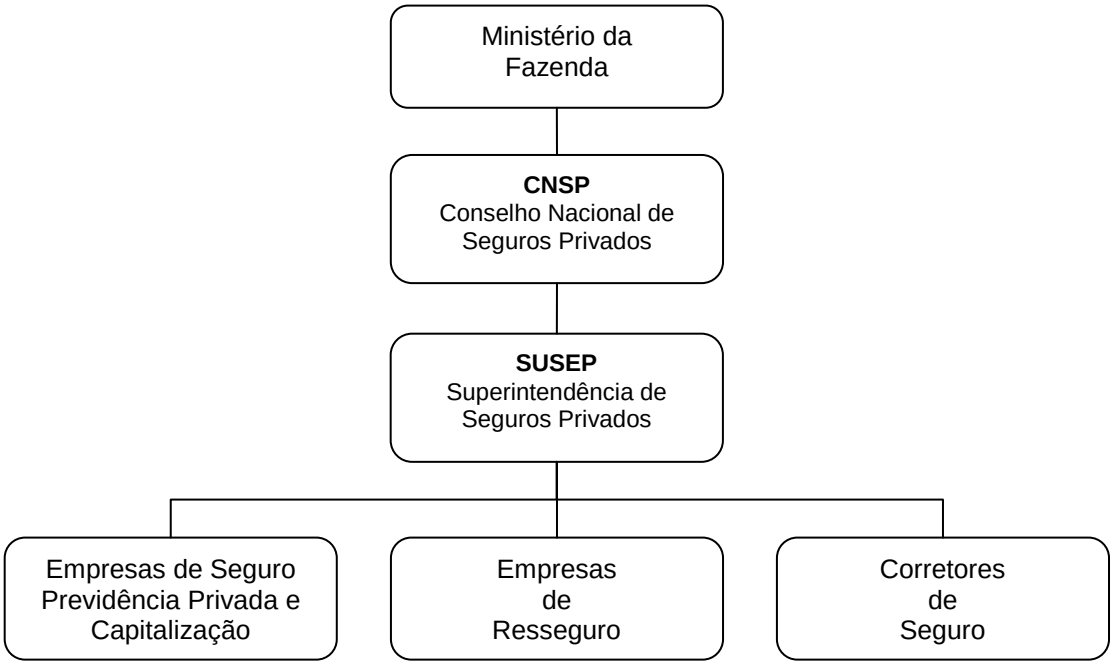


Figura 1: Organograma Sistema Nacional de Seguros Privados
Fonte: (FENASEG, 2010)

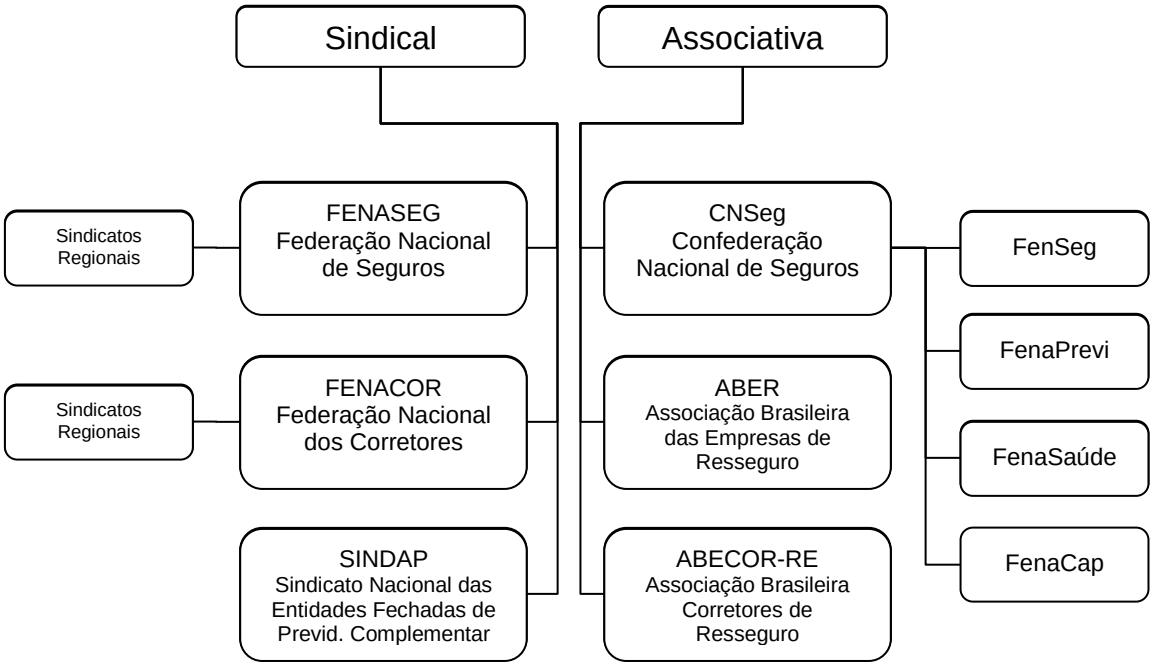


Figura 2: Representação Institucional Sistema Nacional de Seguros Privados
Fonte: (FENASEG, 2010)

Hoje o mercado segurador brasileiro possui 92 ramos, os quais são divididos em 16 grupos que são separados em quatro grandes segmentos: seguros gerais, seguro-saúde, pessoas e capitalização. Assim, o segmento de seguros gerais é composto

por 12 grandes grupos, perfazendo um total de 77 ramos. Esse segmento é responsável por todos os seguros de cobertura de riscos, onde bens e propriedades são envolvidos e consequentemente as responsabilidades inerentes aos mesmos. Já o segmento de seguro-saúde, cuja principal característica é assegurar às pessoas o acesso à medicina particular – hospitais, clínicas e profissionais especializados – é dividido em dois ramos: seguro-saúde individual e seguro-saúde grupal. O segmento de pessoas é integrado por 12 ramos e é responsável por todas as operações relativas ao seguro de vida em geral, formação de pecúlio e da complementação de aposentadoria. Por fim, o segmento de capitalização oferece instrumento que auxilie a população no esforço de constituição de reservas financeiras de curto e longo prazo para a formação de poupança (CNSEG, 2010).

Economicamente o mercado segurador tem crescido e com desempenho além das expectativas. No ano de 2009, o marcado arrecadou mais de R$100 bilhões em prêmios, contribuições e títulos de capitalização, representando um crescimento de 14,91% em relação ao ano anterior. Fazendo um levantamento entre os anos de 2004 a 2009, a produção do mercado segurador no Brasil registrou crescimento acumulado de 82,98%.

Se avaliarmos apenas o segmento de seguros gerais, foi registrado um crescimento acumulado de 66,24%, passando de uma produção de R$19,81 bilhões em 2004, para R$32,94 bilhões em 2009. Destaque para os riscos financeiros, com uma produção individual de R$235 milhões em 2004 passando para R$869 milhões em 2009, obtendo um alto crescimento acumulado no período (CNSEG, 2010).

O crescimento do mercado segurador dos últimos anos tem sido acompanhado pelo aprimoramento dos processos de negócio das empresas e de seus sistemas de informação. O grande responsável é o rápido desenvolvimento do mercado que tem se tornado mais e mais exigente com o passar do tempo. Fato também que tem contribuído para tal aprimoramento é o aumento da complexidade dos negócios do mercado segurador brasileiro. Os investimentos em tecnologia e segurança vem ganhando representatividade significativa dentro do orçamento da companhias do mercado segurador brasileiro, buscando melhor eficácia e eficiência na implementação e monitoramento de controles internos. Com a publicação da Circular SUSEP № 249 de 20 de Fevereiro de 2004, que determina que todas as empresas do mercado segurador, implementem controles internos para todas as suas operações, para seus sistemas de informações e do cumprimento das normas

legais e regulamentares aplicáveis às sociedades desse mercado (SUSEP, 2004), a necessidade da utilização da Tecnologia da Informação, e consequentemente da Segurança da Informação, é evidenciada. Os controles internos devem ser efetivos e consistentes com a natureza, a complexidade e o risco das operações realizadas. Definir as atividades e os níveis de controle para todos os negócios, estabelecer os objetivos dos mecanismos de controles e seus procedimentos, verificar sistematicamente a adoção e o cumprimento desses procedimentos definidos, avaliar continuamente os diversos tipos de riscos associados às atividades da sociedade, acompanhar e implementar as política de conformidade de procedimentos, implantar política de prevenção contra fraudes, implantar política de subscrição de riscos, são apenas algumas das exigências da circular 249 (SUSEP, 2004).

2.2. RISCO

Historicamente o conceito e uso do termo risco são amplos, variados e tem sofrido mudanças ao longo do tempo. Já no século XII foram registrados diferentes termos para o mesmo fim até a utilização da expressão “risco” no século XVI propriamente dito (SPINK, 2001). A utilização da palavra risco na língua portuguesa ocorreu em meados do século XV, havendo registro do francês *risque* no século XVI, ambos provavelmente tomados do italiano *risco* que é uma variação de *rischio,* no século XIII segundo Luhmann (*apud* LIEBER e LIEBER, 2002, p. 71). Luhmann ainda mostra que a definição de risco, apesar do seu uso remoto, é utilizada como uma forma de seguro ainda nos contratos de navegação da antiga Mesopotâmia.

Na língua portuguesa, assim como na língua italiana, a palavra risco deu origem a outras derivações para expressar situações diversas. *Risicare,* que deu origem ao termo mais moderno *rischiare,* cujo sentindo é arriscar ou ousar. Expressão muito utilizada em jogos desde a antiguidade dos tempos.

Esse sentindo positivo do termo risco é utilizado em padrões de mercado como em um dos primeiros trabalhos voltados para o gerenciamento de risco, a AS/NZS 4360:1995, que teve sua primeira versão publicada em 1995. Após duas revisões, uma em 1999 e por fim em 2004, a AS/NZS 4360:2004 tem como definição para risco qualquer chance de algum acontecimento que poderá trazer impacto nos objetivos. É fato que este possível impacto não necessariamente possui uma

conotação negativa, muito pelo contrário, poderá ser positivo (OB-007 COMMITTEE, 2004). Paralelamente outros padrões de mercado foram desenvolvidos, também com o foco para tratamento de risco, como por exemplo, *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) que em 2001 iniciou trabalhos específicos para a composição de uma estrutura para a melhora do tratamento na questão gerenciamento de risco corporativo. Não diferente do mencionado na AS/NZS 4360:2004 Gestão de Risco, o COSO também ressalta a necessidade de trabalhar risco em seu sentido positivo. Os eventos de impacto positivo podem contrabalançar os de impacto negativo ou podem representar oportunidades, que por sua vez representam a possibilidade de um evento ocorrer e influenciar favoravelmente a realização dos objetivos, apoiando a criação ou a preservação de valor (COSO, 2007). Por se tratar de um assunto de interesse global, gerenciamento de risco vem crescendo ao longo do tempo e com ele a evolução dos padrões de mercado. A ISO/IEC 27005:2008 detalha especificamente o tratamento da gestão de riscos de Segurança da Informação, onde risco é definido como a possibilidade de uma determinada ameaça a explorar as vulnerabilidades de um ativo ou conjunto de ativos de segurança (ISO/IEC, 2008).

Já a ISO/IEC 31000:2009 foi desenvolvida por profissionais de excelência de todo o mundo, com origem em diversas disciplinas e indústrias. O padrão tem como principal objetivo nortear as organizações e prover uma plataforma comum para a gestão de diferentes tipos de riscos, com sua fonte independente do tamanho da organização, de seu tipo, complexidade, estrutura, atividade ou localidade.

Na Austrália, a ISO/IEC 31000:2009 Gestão de Riscos – Princípios e Diretrizes foi adotada e conhecida oficialmente como AS/NZS ISO 31000:2009 Gestão de Riscos – Princípios e Diretrizes. O novo padrão de mercado substitui a tão reconhecida e utilizada AS/NZS 4360:2004 Gestão de Risco (GLOBAL, 2011). Fundamentalmente o processo para a gestão de riscos apresentado pela ISO/IEC 31000:2009 é o mesmo utilizado pela AS/NZS 4360:2004. Em sua essência, a ISO/IEC 31000:2009 representa a versão melhorada da versão Australiana, onde alguns conceitos básicos foram removidos e outros melhor definidos. Acompanhando a ISO/IEC 31000:2009, a ISO/IEC 73:2009 Gestão de Riscos – Vocabulário apresenta todos os termos importantes para apoiar a estrutura apresentada em ISO/IEC 31000:2009 (ISO/IEC, 2009).

> "...Risco
> Efeito da incerteza nos objetivos.
> Nota 1: Um efeito é um desvio em relação ao esperado – positivo e/ou negativo
> Nota 2: Os objetivos podem ter diferentes aspectos (tais como metas financeiras, de saúde e segurança e ambientais) e podem aplicar-se em diferentes níveis (tais como estratégico, em toda organização, de projeto, de produto, e de processo)..." (ABNT, 2009)

Com sua definição variada indo desde simplesmente a possibilidade de perda e dano (THO, 2005) até, como sendo o efeito da incerteza nos objetivos (ABNT, 2009), o fato é que a literatura mostra que as diferentes definições convergem para a preservação do valor, ou seja, buscar uma forma de utilização dos impactos positivos para balancear os possíveis impactos negativos. Assim, favorecendo a realização dos objetivos da corporação.

As corporações buscam compreender sua natureza, como mensurá-los e avaliar suas consequências para que seja possível converter o incerto em possíveis ganhos.

O mercado segurador possui toda a base conceitual do cálculo do risco na ideia de que o efeito trás o incerto para o processo decisório nas empresas e indivíduos. O mercado possui variadas técnicas para sua medição e podemos dizer que sua grande maioria converge para um esforço de converter tais incertezas em segurança.

Para qualquer que seja a operação financeira, a associação de riscos é inevitável e certa. Podemos dizer ainda que risco tem um conceito multidimensional e está dividido em quatro grandes dimensões (DUARTE JR., 1996): risco de mercado, risco de crédito, risco legal e risco operacional, conforme mostrado na Figura 3 abaixo.

Figura 3: As quatro dimensões do risco
Fonte: (DUARTE JR., 1996)

2.2.1. Risco de Mercado

Todo risco de perda em decorrência de variações em variáveis econômicas e financeiras, chamamos de risco de mercado. Essas variações podem ser taxas de juros, câmbio, *commodities* e preços de ações. O risco de mercado depende do preço do ativo mediante as condições de mercado. Ainda pode ser definido como:

> "...como uma medida da incerteza relacionada aos retornos esperados de um investimento em decorrência de variações em fatores de mercado como taxas de juros, taxas de câmbio, preços de commodities e ações." (DUARTE JR., 2010)

Podemos dividir risco de mercado em diferentes modalidades, como o risco de taxa de juros, risco cambial, risco de preço de ações e risco de *commodities*. A partir dessa classificação o risco de mercado fica composto por quatro variáveis geradoras de risco. Cada modalidade representa o risco de ocorrerem perdas em função de oscilações na variável em questão.

2.2.2. Risco de Crédito

Podemos dizer que crédito refere-se à atividade de colocar um valor a disposição de um tomador de recursos sob a forma de empréstimo ou financiamento, mediante compromisso de pagamento em data futura. Assim, o risco de crédito é definido como a possível falha do cumprimento desse compromisso futuro, ou seja, da possibilidade de perdas quando o contratante não honra seus compromissos. Entendemos que todas as perdas provenientes do risco de crédito estão relacionadas aos recursos que não mais serão recebidos.

2.2.3. Risco Legal

Este está diretamente relacionado com as possíveis perdas por falta de suporte legal de contratos. Podemos incluir dentro de riscos legais, perdas por ilegalidade, falta de representatividade por uma das partes, insolvência, etc.

2.2.4. Risco Operacional

O risco operacional é aquele que resulta da execução dos processos de negócio da corporação. Diversos riscos são incluídos nessa categoria, já que são riscos que colocam em causa a execução normal do negócio. Está relacionado a possíveis perdas como resultado de sistemas e/ou controles inadequados, falhas de gerenciamento e erros humanos (DUARTE JR., 1996). Ainda, podemos definir risco operacional como:

> "... a possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos." (BRASIL, 2010)

Ainda, a Resolução 003380 do Banco Central do Brasil nos mostra como eventos de risco operacional:

> "... § 2º Entre os eventos de risco operacional, incluem-se:
>
> I. Fraudes internas;
> II. Fraudes externas;
> III. Demandas trabalhistas e segurança deficiente do local de trabalho;

IV. Práticas inadequadas relativas a clientes, produtos e serviços;
V. Danos a ativos físicos próprios ou em uso pela instituição;
VI. Aqueles que acarretem a interrupção das atividades da instituição;
VII. Falhas em sistemas de tecnologia da informação;
VIII. Falhas na execução, cumprimento de prazos e gerenciamento das atividades na instituição.” (BRASIL, 2010)

Podemos ainda dividir risco operacional em três grandes áreas (DUARTE JR., 1996):

a) Risco organizacional – Organização ineficiente com sua administração sem objetivos bem definidos em longo prazo. Responsabilidades não delineadas corretamente, vazamento de informação sensível ao negócio, fraudes internas, etc.
b) Risco de operações – Sobrecarga de sistemas de informação, como telefonia e computacional. Deficiência no processamento e armazenamento de dados. Falta de verificação e/ou confirmação das informações pertinentes ao negócio, possibilitando erros e fraudes.
c) Risco de pessoal – Mão de obra não qualificada, sem motivação, colaboradores em zona de conforto.

2.2.4.1. Exigências Regulatórias

Devido ao grande número de empresas norte-americanas passarem pelo processo de concordada nos últimos tempos, os órgãos reguladores de proteção aos investidores de diversas nacionalidades, estabeleceram formalmente a responsabilidade gerencial para os gestores das corporações. Buscando a transparência gerencial e melhor *accountability* (prestação de contas), esses requisitos formam um conjunto de ações que chamamos de governança corporativa.

> “Governança Corporativa é o sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre proprietários, Conselho de Administração, Diretoria e órgãos de controle. As boas práticas de Governança Corporativa convertem princípios em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor da organização,

> facilitando seu acesso a recursos e contribuindo para sua longevidade." (CORPORATIVA, 2010)

A partir de julho de 2002 a Lei *Sarbanes-Oxley* entrou em vigor nos Estados Unidos buscando fechar mais ainda a regulamentação sobre o setor contábil do país. O SOX estende os poderes às empresas estrangeiras do setor que possuam clientes americanos. A partir de sua divulgação, os executivos das corporações devem avalizar as demonstrações contábeis e estão sujeitos às sanções se conscientemente cometerem qualquer fraude. Desta forma, é de responsabilidade desses executivos (administradores) identificar, documentar e testar os processos mais críticos.

No Brasil, através da utilização de normas de governança corporativa e leis como a 6.404 de 1976 (alterada pela Lei 10.303), as empresas de capital aberto são obrigadas à transparência fiscal de forma que assegura-se maior efetividade aos mecanismos de governança em território nacional. Ainda para o Brasil, o Código de Melhores Práticas do Instituto Brasileiro de Governança Corporativa – IBGC estabelece que o executivo seja o responsável pela criação de sistemas de controles internos com a função de organizar e monitorar o fluxo de informações corretas, reais e completas sobre a sociedade. Essas informações deverão ser de natureza financeira, operacional e legal que apresentem fatores importantes de risco. Esses mecanismos devem, ainda segundo o IBGC, ter sua efetividade revista anualmente (FERREIRA, 2006).

2.3. TAXONOMIA

Derivada de uma ramificação da Biologia, a que classifica lógica e cientificamente os seres vivos, taxonomia vem do grego taxis=ordem e onoma=nombre.

A taxonomia refere-se a qualquer conjunto de classificação que seja nativo, ordenando a informação de alguma maneira. Uma das mais conhecidas formas de taxonomia é a classificação de organismos vivos, realizada por Karl Von Linné, no ano de 1735. Karl usou o conceito de taxonomia para a criação de uma classificação para seres vivos, dividindo-os em grupos com características comuns. A Figura 4 mostra um exemplo desse tipo de classificação de 1735.

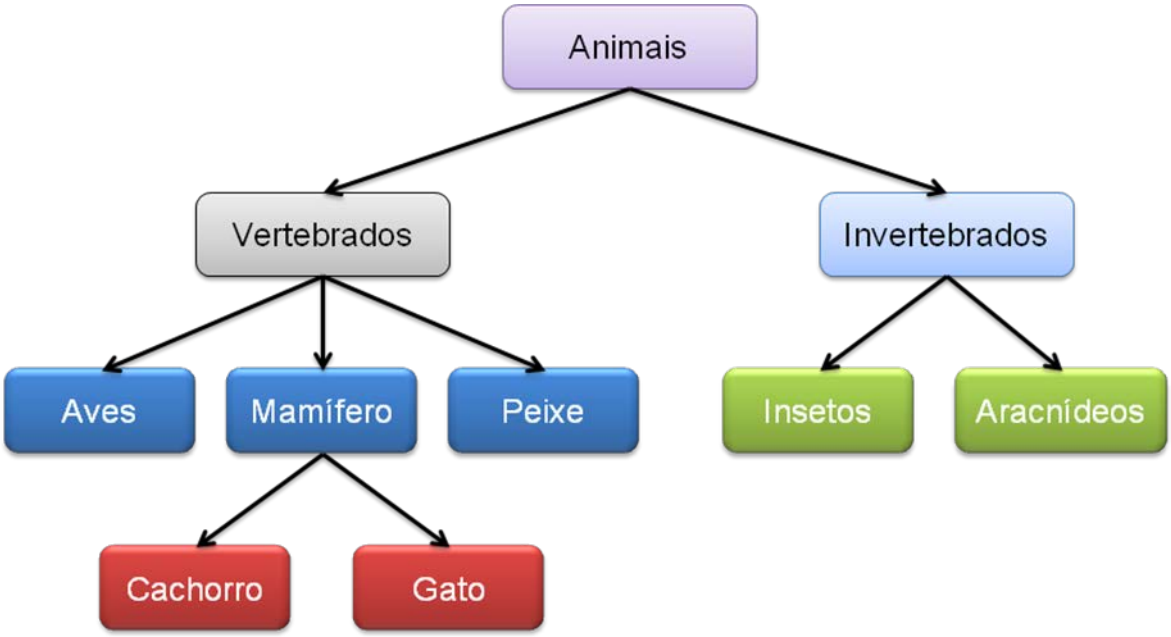


Figura 4: Ilustração de taxonomia de Karl Von Linné
Fonte: (TERRA, 2010)

> "A taxonomia é um sistema para classificar e facilitar o acesso à informação, e que tem como objetivos: representar conceitos através de termos; agilizar a comunicação entre especialistas e entre especialistas e outros públicos; encontrar o consenso; propor formas de controle da diversidade de significação; e oferecer um mapa de área que servirá como guia em processos de conhecimento. É, portanto, um vocabulário controlado de uma determinada área do conhecimento, e acima de tudo um instrumento ou elemento de estrutura que permite alocar, recuperar e comunicar informações dentro de um sistema, de maneira lógica." (TERRA, 2010)

Ainda, a taxonomia, é uma ciência de identificação que pode ser utilizada para o desígnio de conjuntos de termos representativos de uma área, estruturados de forma hierárquica.

Apesar de ter nascido de uma derivação da biologia, seu uso no âmbito digital está diretamente relacionado com formas de criação da informação. As taxonomias são voltadas à organização das informações, de forma que sua recuperação seja eficaz. Essa organização pode ser visualizada na Figura 5, onde após o desenvolvimento de uma taxonomia os termos foram organizados de forma lógica e interdependente, tornando sua busca facilitada.

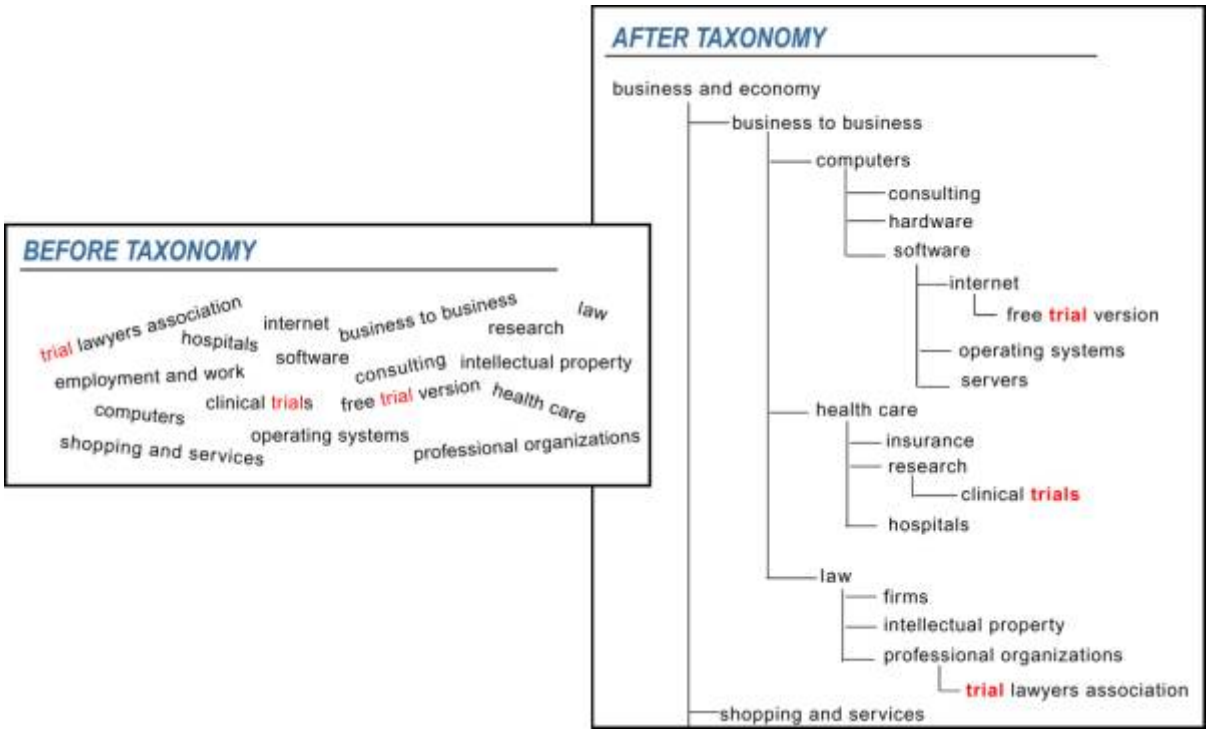


Figura 5: Antes e depois da criação de uma taxonomia
Fonte: (DUTRA e BUSCH, 2003)

De forma geral, todas as disciplinas científicas podem se beneficiar ao utilizar qualquer que seja o método de organização da informação e para segurança da informação não poderia ser diferente. A utilização de um esquema de classificação é indiscutivelmente importante: a taxonomia faz-se necessária para que um vocabulário comum seja criado e compartilhado entre partes interessadas, sejam da mesma área geográfica, área de interesse ou mesmo de atuação. A literatura mostra que esforços e interesse para trabalhar com taxonomias no âmbito computacional surgiram na década de 1970, com a tentativa de classificar falhas de segurança em sistemas operacionais. A pesquisa foi conduzida através do projeto denominado RISOS (*Research Into Secure Operating Systems*) que em seu relatório final descreve sete categorias de falhas de segurança para sistemas operacionais: validação de parâmetro incompleta, validação de parâmetro inconsistente, compartilhamento implícito de dados confidenciais/privilegiados, validação assíncrona/serialização inadequada, identificação/autenticação/autorização inadequada, proibição/limite violável e erro lógico explorável (ABBOTT, CHIN, *et al.*, 1976).

A utilização de metodologias que envolvem algum tipo de taxonomia para a identificação de riscos é evidenciada através de trabalhos do *Software Engineering*

Institute - SEI da *Carnegie Mellon University* em Pittsburgh na Pensilvânia. O relatório técnico CMU/SEI-93-TR-6 (CARR, KONDA, *et al.*, 1993), datado de 1993, mostra já uma iniciativa de identificação de riscos com base em uma taxonomia conceituada segundo *The Institute of Electrical and Electronics Engineers – IEEE* (IEEE, 1990), que descreve um método para facilitar a sistemática de identificação de riscos associados ao desenvolvimento de software. O método consiste em questionário taxonômico (*Taxonony-based questionnaire – TBQ*) que como resultado organiza o desenvolvimento de software em três níveis de riscos: classe, elemento e atributo. A Figura 6 mostra a macro taxonomia para risco em desenvolvimento de software.

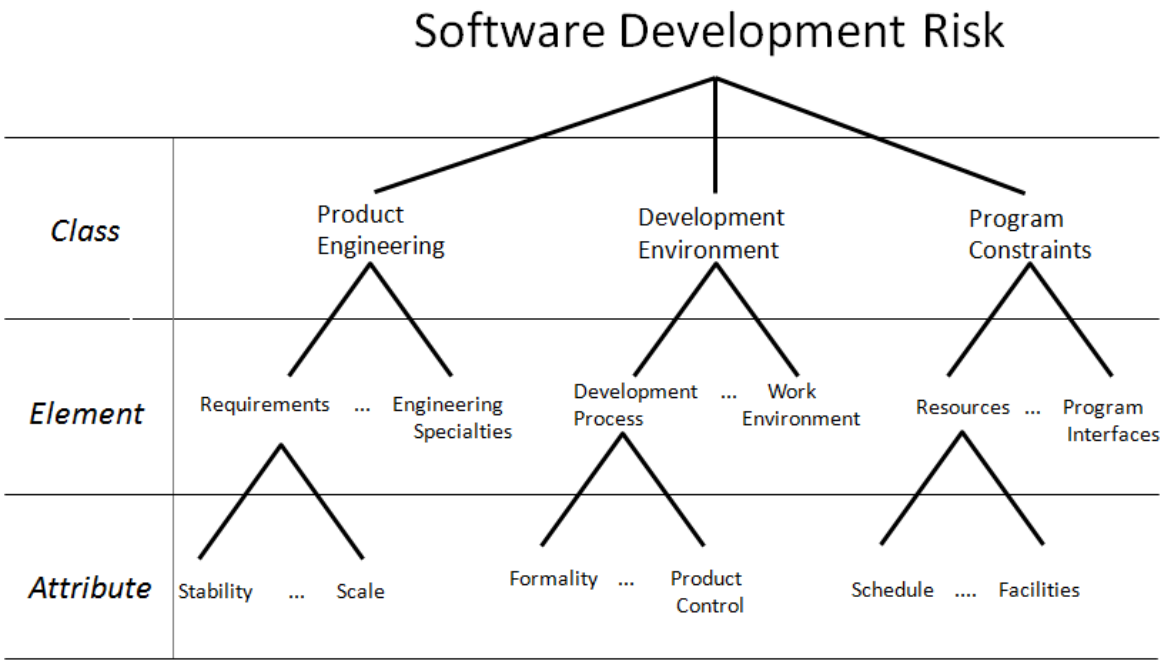


Figura 6: Taxonomia para risco em desenvolvimento de software
Fonte: (CARR, KONDA, *et al.*, 1993)

Em 2005, ainda pelo *Software Engineering Institute – SEI,* a representação de risco operacional através de uma estrutura taxonômica é mostrada segundo o relatório técnico CMU/SEI-2005-TR-036 (GALLAGHER, CASE, *et al.*, 2005) que apresenta uma metodologia de identificação e classificação de riscos corporativos em seu aspecto puramente operacional. O trabalho detalha as principais fontes de riscos associadas com a missão, processos de trabalho e restrições de um ambiente operacional e também estabelece uma estrutura para a representação dos riscos

operacionais, agrupando-os em diferentes classes, elementos e atributos. O levantamento dos riscos em questão só foi possível com a utilização de questionários e aplicação de experiência acadêmica e de mercado (GALLAGHER, CASE, *et al.*, 2005). A Figura 7 mostra a macro taxonomia para risco operacional segundo (GALLAGHER, CASE, *et al.*, 2005).

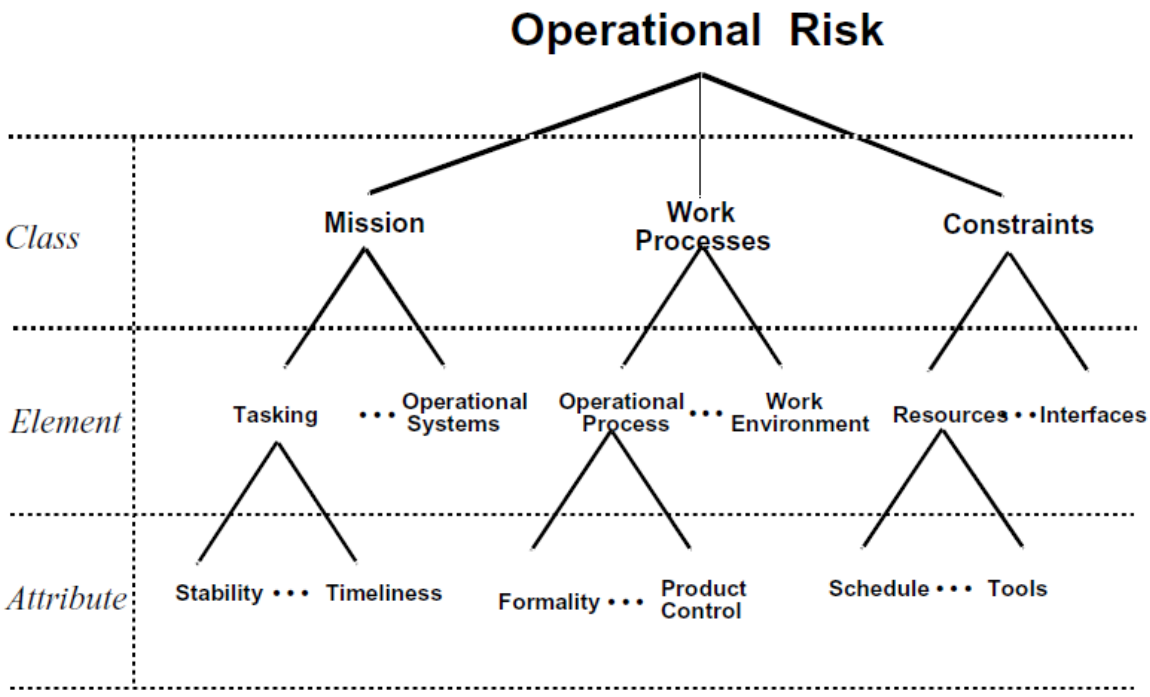


Figura 7: Macro taxonomia para risco operacional
Fonte: (GALLAGHER, CASE, *et al.*, 2005)

Com o suporte dos questionários taxonômicos, conforme mostrado exemplo na Figura 9, o método tem como resultado uma taxonomia mais completa, mostrada na Figura 8.

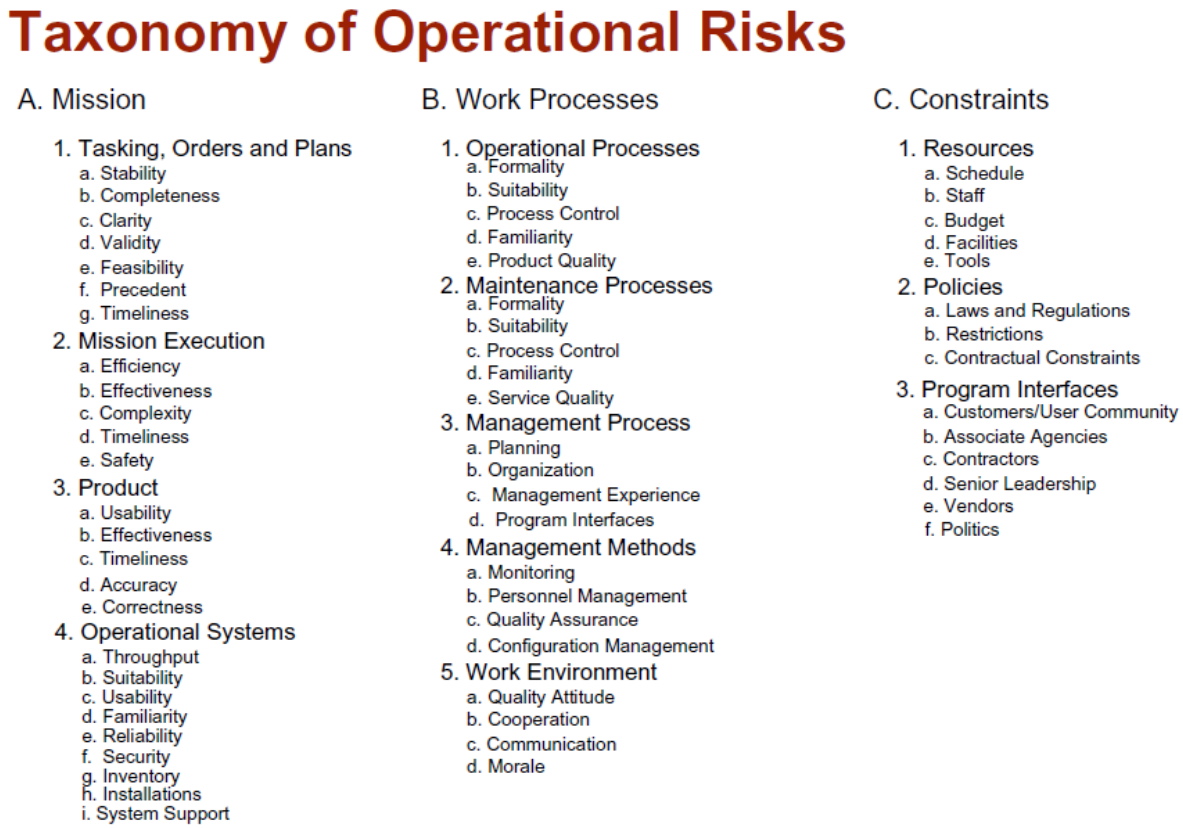
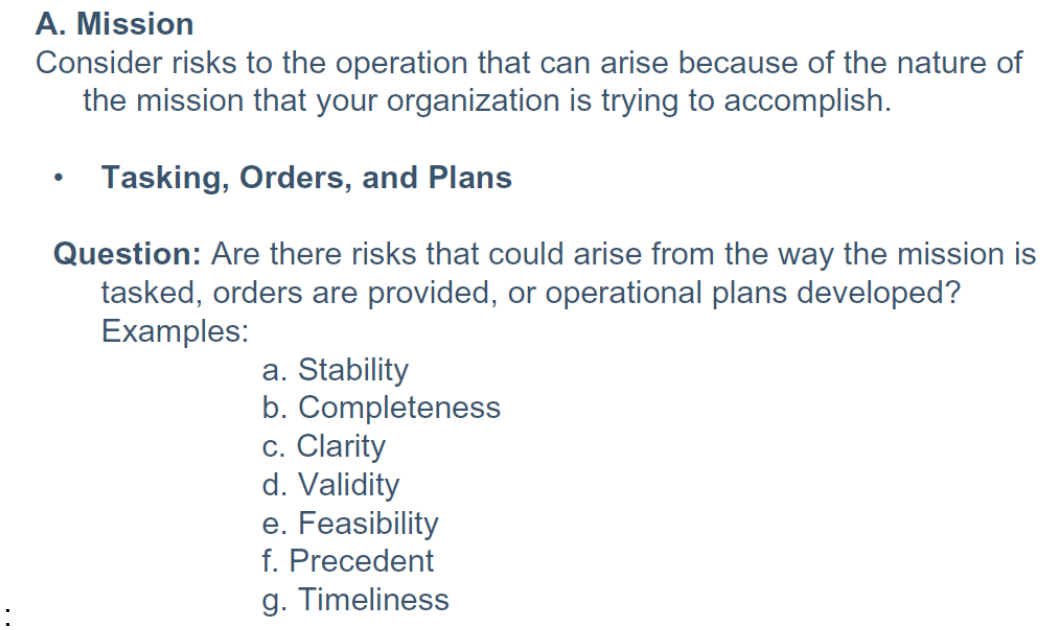


Figura 8: Taxonomia de risco operacional

Fonte: (GALLAGHER, CASE, *et al.*, 2005)



:

Figura 9: Parte do questionário taxonômico

Fonte: (GALLAGHER, CASE, *et al.*, 2005)

De forma geral, conceitualmente, a taxonomia trata-se de uma organização hierárquica; no entanto trataremos a taxonomia de forma corporativa e, portanto, com definições mais específicas. A literatura mostra que existem diversas formas e tipos de taxonomia bem como existem vários métodos de construção dessas estruturas taxonômicas. Segundo Susan Conway (CONWAY e SLIGAR, 2003) existem três tipos de taxonomias aplicadas à ambientes corporativos: taxonomia descritiva, taxonomia para navegação e taxonomia para gerenciamento de dados.

Taxonomia Descritiva

A taxonomia chamada descritiva é representada pela criação de um vocabulário controlado e tem como principal objetivo aperfeiçoar a busca e recuperação da informação. Segue a mesma linha da estrutura de tesauro, com termos significativos para um determinado contexto, possui relações de sinonímia, homonímia, de forma que o usuário, no processo de busca, possa utilizar termos de sua preferência. Não existe a obrigação de uso de apenas um único conjunto de termos, pelo contrário, diversas variantes de palavras, formas, sintaxe, etc.

Taxonomia para Navegação

Com sua organização diferente da taxonomia descritiva, a taxonomia para navegação trabalha com agrupamentos das informações. Essa, por sua vez, é descoberta a partir do comportamento do usuário a partir da utilização de navegadores. Baseada em modelos mentais, na organização da informação e no comportamento do usuário. O importante é que para esse tipo de taxonomia as relações existentes entre termos devem fazer sentindo para seus usuários, não necessitando que tais termos possuam subordinações lógicas.

Taxonomia para Gerenciamento de Dados

Busca formar conjuntos de dados que sejam controlados, com atributos específicos. Tem como objetivo garantir o compartilhamento de dados entre certos grupos da organização. Segue a mesma linha da taxonomia descritiva, mas sem o intuito de promover acesso a toda informação produzida na organização. Sem essa taxonomia compartilhada, a corporação corre o risco de criação de silos de dados e para alguns casos, de conhecimento. A disposição de seus componentes pode ser representada

de várias formas, utilizando-se de uma estrutura hierárquica ou não. No entanto, esta lista de termos deve ser uma lista de termos autorizados.

Já para (BLACKBURN, 2006), as estruturas taxonômicas corporativas, são estruturas hierárquicas divididas em três tipos: por assunto, por unidade de negócio e funcional.

Taxonomia por Assunto

A estrutura taxonômica por assunto utiliza de vocabulário controlado e organiza seus componentes por assuntos do mais geral ao mais específico, geralmente em ordem alfabética. Este tipo de estrutura exige um conhecimento da área por parte do usuário.

Taxonomia por Unidade de Negócio

O foco desse tipo de taxonomia é a unidade de negócio da corporação, facilitando sua utilização para aqueles que conhecem tal estrutura organizacional. Sua grande desvantagem está associada às modificações que a estrutura corporativa possa sofrer, dificultando trabalhar com documentos gerenciados ou compartilhados por várias unidades de negócio.

Taxonomia por Função

A taxonomia funcional toma como base todas as funções e atividades desenvolvidas pela organização. Os processos de negócio da organização são adotados para se estabelecer tal taxonomia.

Se compararmos os diversos tipos de taxonomia apresentadas por (CONWAY e SLIGAR, 2003) e (BLACKBURN, 2006) podemos dizer que as semelhanças são grandes e diversas. Taxonomia descritiva e por assunto, onde ambas utilizam-se de vocabulários controlados e focam na eficiência da busca e recuperação da informação. Assim como a taxonomia de gerenciamento de dados e funcional tem como objetivo a representação da informação segundo áreas específicas da organização. A taxonomia no ambiente corporativo, usada como método de representação da informação disponível na organização, não deve ser contemplada por somente um tipo e sim fazer uso de metodologias diferentes que unidas possam

suportar os diversos tipos de informação bem como a diversidade da própria organização.

2.4. SEGURANÇA DA INFORMAÇÃO

2.4.1. Introdução

Neste capítulo serão introduzidos alguns conceitos e princípios de Segurança da Informação os quais serão utilizados nesta dissertação. Buscando prover a base para apoiar o uso de uma classificação de riscos relacionados à própria segurança da informação em empresas do mercado segurador brasileiro. Na primeira parte descreveremos o que é Segurança, seguido por seus princípios básicos e então seus diferentes tipos e domínios de atuação.

2.4.2. Definindo Segurança

Pode-se definir Segurança, de acordo com o dicionário Aurélio (FERREIRA, 1999), como:

> Segurança. [De segurar + -ança] S. f.
> 1. Ato ou efeito de segurar: Mal entrou no avião, foi apertando o cinto de segurança. [Sin., p. us.: seguração.]
> 2. Estado, Qualidade ou condição de seguro.
> 3. Condição daquele ou daquilo em que se pode confiar: Compre estas ações: apresentam muita segurança.
> 4. Certeza, firmeza, convicção: Respondeu às perguntas do mestre com muita segurança.
> 5. Confiança em sim mesmo; autoconfiança: Vive atrás da opinião alheia, não tem segurança.
> 6. Caução garantia; seguro: Dou-lhe a segurança de minha amizade.
> 7. Protesto, afirmação. [Sin., p. us., nessas acepç: segureza, seguridade.]
> 8. Prenhez das fêmeas dos quadrúpedes.
> 9. Bras. V. alfinete de segurança. S. 2 g.
> 10. Bras. Pessoa encarregada da segurança pessoal de alguém, ou de empresa, etc. [Cf. guarda-costas (2).]

Para que a definição de segurança fique completa é necessário a definição do termo seguro, que ainda de acordo com o dicionário Aurélio (FERREIRA, 1999) temos:

> Seguro [Do lat. Securu] Adj.
>
> 1. Livre de perigo: Está em lugar seguro.
> 2. Livre de risco; protegido, acautelado, garantido: “É a guerra aquela calamidade composta de todas as calamidades, em que não há mal algum, que ou se não padeça, ou se não tema; nem bem, que sea próprio, e seguro. O pai não tem seguro o filho, o rico não tem segura a fazenda” (P.^{e} Antônio Vieira, Sermões, XIV, p.9).
> 3. Isento de receios; corajoso, afoito.
> 4. Que não hesita, ou não vacila; firme: É homem seguro em suas atitudes.
> 5. Certo, convencido, convicto: Está seguro de suas razões.
> 6. Prudente, ponderado, comedido, cauteloso: É muito seguro nos seus empreendimentos.
> 7. Que tem autoconfiança: Seguro de si, compareceu perante o juiz.
> 8. Em quem se pode confiar; constante, leal.
> 9. Certo, indubitável, incontestável: “A impunidade é segura, quando a cumplicidade é geral.” (Marquês de Maricá, Máximas, Pensamentos e Reflexões, p. 28); São seguros os dados fornecidos pelo computador.
> 10. Eficaz, eficiente: A empresa só progredirá com uma programação segura; É um remédio seguro.
> 11. Preso, fixo, firme: A prateleira está bem segura.
> 12. Preso, encarcerado, custodiado.
> 13. Robusto, rijo; firme: É senhora já idosa, mas ainda segura.
> 14. V. avaro (1).
> 15. Dize do tempo bom, estável, sem probabilidade de chuva: Há três semanas o tempo está seguro.
> 16. Bras. S. Diz-se do animal prenhe: vaca segura. S. m.
> 17. Contrato pelo qual, mediante cobrança de pagamento periódico, uma das partes se obriga a pagar uma indenização a outra na ocorrência de determinado evento como, p. ex., incêndio, roubo, acidente, morte, etc. [Cf., nesta acepç., apólice(2), prêmio(4), risco^{2}(3) e sinistro(7).]
> 18. A indenização paga num seguro (17): Fulano já recebeu o seguro pelo roubo de seu carro.
> 19. V. salvaguarda (2).
> 20. Registro (10).
> 21. Segurança (6).
> 22. Seguradora: O seguro pagou a batida do carro – Adv.

> 23. Com segurança; seguramente: Joga seguro; Aquele cirurgião opera rápido e seguro. – Seguro de vida. Seguro (17) que prevê indenização a sobrevivente(s) indicado(s), em caso de morte do segurado.

A norma ABNT ISO/IEC 27002:2005 (27002:2005, 2005) define informação como "... um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização..." e a mesma norma define segurança da informação como sendo:

> "Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio." (27002:2005, 2005).

2.4.3. Princípios básicos para Segurança da Informação

Tópico fascinante, segurança permeia por diferentes visões e aqui mostraremos seus princípios de acordo com três diferentes pontos de vista: - A tríade CID (Confidencialidade, Integridade e Disponibilidade), RICE (*Responsability, Integrity, Trust and Ethicaly*) e Hexágono Parkeriano. Buscamos uma melhor compreensão de onde esses princípios se completam e/ou unem-se.

2.4.3.1. A tríade CID

Os princípios Confidencialidade, Integridade e Disponibilidade quando combinados formam a tríade CID. O padrão ABNT NBR ISO/IEC 27002 (27002:2005, 2005) é um bom exemplo de onde podemos encontrar a aplicação da tríade CID. Esse padrão de mercado consiste na recomendação de práticas de segurança para o gerenciamento de segurança da informação.

Confidencialidade

Assegura que toda e qualquer informação seja somente acessível por quem de direito, ou seja, qualquer recurso (computacional ou não) que tenha a devida autorização para tanto (PFLEEGER, 2006). A confidencialidade pode ser alcançada através de níveis de confidencialidade onde mecanismos de proteção devem garantir o acesso à informação por entidades não autorizadas. Tipicamente para

garantir níveis satisfatórios de confidencialidade, técnicas de criptografia são utilizadas no tráfego e armazenamento da informação (HARRIS, 2010).

Integridade

Integridade deve garantir que toda e qualquer informação seja alterada somente por entidades com autorização para tanto (PFLEEGER, 2006). Mecanismos de segurança devem prevenir qualquer modificação da informação mesmo por aquelas entidades sem autorização que tenham acesso a ela.

Disponibilidade

Disponibilidade deve garantir que a informação esteja acessível para entidades autorizadas em um tempo razoável. A informação também deve estar em um formato adequado (PFLEEGER, 2006). Mecanismos de segurança devem ser utilizados para garantir a proteção contra ameaças internas/externas as quais poderiam afetar a disponibilidade e produtividade do recurso em questão (HARRIS, 2010).

2.4.3.2. RICE

Uma proposta de expansão da tríade CID foi feita por Dhillon e Backhouse (DHILLON e BACKHOUSE, 2000) onde novos princípios: responsabilidade, integridade, confiança e ética (RICE), são adicionados na tratativa de assuntos relacionados à segurança da informação. Segundo Dhillon (DHILLON e BACKHOUSE, 2000), a tríade CID é muito restrita e aplica-se basicamente para informação como dado, ou seja, observações documentadas ou resultados de uma medição. Ainda de acordo com Dhillon (DHILLON e BACKHOUSE, 2000) os princípios de segurança da informação devem se referir ao uso e interpretação da informação de acordo com normas existentes da corporação.

Afirma Dhillon (DHILLON e BACKHOUSE, 2000) que com a utilização do RICE é possível olhar para problemas de segurança através de uma perspectiva mais holística e alinhada com o ambiente corporativo.

Responsabilidade

Significa conhecimento e entendimento das regras da corporação. Responsabilidade é ponto focal para organizações com novas estruturas de gerenciamento e ambiente altamente suscetível a mudanças rápidas.

Integridade

Integridade significa necessidade de filiação. O sentimento de integridade como membro integrante da corporação e também sua lealdade para com a corporação é de extrema importância atualmente. A informação possui grande valor e é o ativo mais valioso de qualquer empresa nos dias de hoje e em função disso, somente membros da corporação que se sentem alinhados com a corporação devem ter acesso á mesma.

Confiabilidade

Confiança no lugar de controle. Com a nova geografia mundial corporativa, onde o controle próprio é mais importante do que controles externos e responsabilidades são mais efetivas que supervisão, sistemas mútuos de confiança devem existir. O nível de confiança para as ações de cada colaborador deve estar de acordo com as políticas e normas da corporação e padrões de comportamento do mesmo. Finalmente, o colaborador deve estar seguro de que sua privacidade não será comprometida por controles restritivos em excesso.

Ética

Ética no lugar das regras. Essas se aplicam para circunstâncias previsíveis e não serão utilizadas em situações novas e dinâmicas. Por isso é importante que o colaborador aja de acordo com práticas de ética. Essas se referem a normas e comportamentos informais.

2.4.3.3. Hexágono Parkeriano

Parker (PARKER, 2002) propõe um *framework* (Hexágono Parkeriano) em substituição à tríade CID. Este consiste basicamente em seis elementos de segurança: disponibilidade, utilidade, integridade, autenticidade, confidencialidade e posse. Segundo Parker (PARKER, 2002) os princípios apresentados pela tríade CID

tem como função principal proteger somente computadores e sistemas de rede e não as aplicações desses sistemas. Parker (PARKER, 2002) ainda propõe que não haja conflito entre os seis princípios de seu modelo. Se um princípio de segurança não é levando em consideração, as perdas em potencial poderão surgir quando não levando em consideração tal princípio.

Disponibilidade

Usabilidade da informação para um propósito.

Utilidade

Presteza da informação para um propósito.

Integridade

Informação completa, íntegra e legível.

Autenticidade

Validade, conformidade e veracidade da informação.

Confidencialidade

Observação e distribuição limitada do conhecimento.

Posse

Habilidade de controlar e possuir o uso da informação.

Tabela 1 Tabela comparativa entre Tríade CID, RICE e Hexágono Parkeriano

Tríade CID	RICE	Hexágono Parkeriano
Confidencialidade	**Confidencialidade**	**Disponibilidade**
Integridade	**Integridade**	**Utilidade**
Disponibilidade	**Disponibilidade**	**Integridade**
	Responsabilidade	**Autenticidade**
	Integridade	**Confidencialidade**
	Confiabilidade	**Posse**
	Ética	

Fonte: O autor

2.4.4. Princípios adicionais de segurança

Complementando os princípios básicos de segurança da informação confidencialidade, integridade e disponibilidade, apresentamos alguns elementos adicionais autenticação, autorização e não repúdio. A necessidade desses princípios adicionais é justificada pelo surgimento de ambientes onde o controle total não é alcançado pelas organizações (KRAFZIG, BANKE e SLAMA, 2004).

Identificação

É o ato de reclamar uma identidade.

Autenticação

Autenticação é o ato de comprovar a veracidade da identidade da entidade. É fato que autenticação envolve identificação. Geralmente a identificação é o primeiro passo no processo de autenticação e autorização. Na falta da autenticação os elementos básicos de segurança (tríade CID) não poderão ser implementados, já que tornaria impossível determinar se um recurso foi alterado e/ou exposto por uma entidade autorizada. Consideremos basicamente três tipos de autenticação (PFLEEGER, 2006):

- Autenticação baseada em conhecimento

Tradicionalmente esse conhecimento é algo comumente que somente a entidade a ser autenticada o detém. A forma mais comum de representação desse algo conhecido chamamos de senha que é encontrada no formato de palavra ou frase secreta (UNIVERSITY, 2010).

- Autenticação baseada em fichas ou *tokens*

As fichas são algo que a entidade a ser autenticada possui. Na autenticação baseada em fichas a mesma é solicitada no momento da identificação da entidade.

- Autenticação baseada em biometria

A biometria é algo que a entidade, neste caso o ser humano, a ser autenticada é. Podemos citar como exemplos de biometria a impressão digital, íris dos olhos e palma das mãos.

Autorização

Autorização é o processo de concessão de privilégios a um acesso de uma entidade para um recurso específico.

Não repúdio

Quando falamos de comunicação segura temos que garantir que as entidades de envio e recebimento da informação não podem negar seu envio ou recebimento (SALOMON, 2006).

2.4.5. Domínios de Segurança

O $(ISC)^2$ ((ISC)2) divide segurança da informação em dez domínios de atuação facilitando a compreensão das diversas áreas em que a segurança atua. Esses domínios nos ajudam a ter uma visão com um maior grau de detalhe quando tratando de problemas abrangentes. É fato que em sua atuação, segurança sempre trata com mais de um domínio simultaneamente. Segue uma descrição para cada domínio:

Controle de Acesso

Este domínio é o responsável por examinar todos os mecanismos e métodos utilizados para possibilitar que administradores e/ou gerentes tenham o controle do que se pode acessar por parte das entidades. Também examina a extensão de suas capacidades após sua autenticação e autorização bem como todas as auditorias e monitoramento dessas atividades (HARRIS, 2010).

Alguns dos tópicos cobertos por este domínio são:

- Modelos de segurança para controle de acesso;
- Tecnologias e técnicas de identificação e autenticação;
- Administração de controle de acesso
- Tecnologias de assinatura única.

Criptografia

Domínio responsável por caracterizar métodos e técnicas de modificação da informação original obtendo como resultado algo ilegível de forma que somente a

entidade com o devido acesso tenha capacidade de torná-la legível como em sua forma original.

Alguns dos tópicos cobertos por este domínio são:

- Algoritmos simétricos e assimétricos;
- Infraestrutura de chaves públicas (*Public Infrastructure Key - PKI)*;
- Funções de *hashing*;
- Protocolos de criptografia;
- Assinatura digital.

Governança em Segurança da Informação e Gerenciamento de Risco

Responsável por toda governança em segurança da informação e gerenciamento de risco da corporação. Domínio que busca a identificação de todos os ativos da corporação, determinando os níveis de proteção necessários de acordo com a estratégia corporativa. Também responsável por determinar a previsão orçamentária para que os sistemas de segurança da informação sejam implementados.

Alguns dos tópicos cobertos por este domínio são:

- Classificação da informação;
- Políticas, procedimentos, padrões e guias;
- Levantamento e gerenciamento de risco;
- Treinamento, segurança de pessoal e programas de conscientização.

Leis, Regulamentações, Investigações e Conformidade

Crime digital, legislação vigente e leis. Responsável pelas técnicas de coleta de evidências, investigação e procedimentos específicos. Este domínio também é responsável por desenvolver e implementar o programa de incidentes. Alguns outros tópicos cobertos por este domínio são:

- Tipos de leis e crimes digitais;
- Licenciamento de software;
- Controle de incidentes;
- Gerenciamento de evidências admissíveis em juízo;

Planejamento de Continuidade do Negócio e Recuperação de Desastre

Tendo como principal responsabilidade, esse domínio tem como objetivo a preservação das atividades do negócio em momentos de crise (interrupção do serviço) e/ou desastre. O levantamento e identificação de riscos reais e a implementação de medidas de controle buscando a mitigação desses. Alguns outros tópicos cobertos por este domínio são:

- Identificação de recursos das atividades de negócio;
- Análise de impacto ao negócio (*Business Impact Analysis – BIA)*;
- Previsão de possíveis perdas;
- Gerenciamento de crise;
- Desenvolvimento, implementação e manutenção de plano de continuidade.

Segurança de Rede e Telecomunicações

Responsável por todos os sistemas internos, externos, públicos e privados de comunicação. Estruturas de redes, dispositivos, protocolos, acesso remoto e toda sua administração.

Segue alguns tópicos cobertos por este domínio:

- Modelo de camadas ISO/OSI;
- Tecnologias para redes local, metropolitana e de longa distância;
- Assuntos relacionados a Internet, intranet e extranet;
- Redes virtuais privadas e firewalls;
- Roteadores, pontes e repetidores;
- Topologia de rede e cabeamento;
- Métodos de ataque.

Segurança em Arquitetura e Desenvolvimento

Domínio onde todos os conceitos, princípios e padrões para o desenvolvimento e implementação segura de aplicações, sistemas operacionais e sistemas são examinados. Responsável pela métrica de segurança com base em padrões internacionais e seu significado para as diferentes plataformas da corporação. Alguns outros tópicos para este domínio são:

- Mapeamento de memória;
- Funções *kernel*;

- Arquitetura corporativa;
- Modelos de segurança;
- Modelos de arquitetura;
- Critérios de validação como TCSEC (*Trusted Computer Security Evaluation*), ITSEC (*Information Technology Security Evaluation Criteria*);
- Falhas de aplicações e sistemas.

Segurança em Desenvolvimento de Aplicações

Responsável por examinar os componentes pertencentes a sistemas operacionais e aplicações bem como gerenciar seu desenvolvimento seguro. Tratando também do ciclo de vida para software, controle de mudanças e segurança de aplicação.

Alguns dos tópicos cobertos por este domínio são:

- Mineração de dados;
- Melhores práticas de desenvolvimento e seus riscos;
- Vulnerabilidade de componente de software;
- Código malicioso.

Segurança em Operações

Trata das técnicas de controles relacionados à pessoal, *hardware*, sistemas e seu monitoramento e auditoria. Alguns outros tópicos abordados por este domínio são:

- Responsabilidades administrativas pertinentes a pessoal e rotação de funções;
- Mantenedor de conceitos de antivírus, treinamento, auditoria e atividades de proteção de recursos;
- Controles de prevenção, detecção, correção e recuperação;
- Padrões e conceito de *due care*;

Segurança Física

Domínio que examina ameaças, riscos e medidas de controle para proteger as dependências físicas da corporação, seu *hardware*, dados, mídia e pessoal. Envolvendo métodos de controle de acesso físico, procedimentos de segurança e seleção de pessoal. Alguns outros tópicos cobertos por este domínio:

- Métodos de autorização, restrição de áreas e seus controles;
- Detecção de movimento, sensores e alarmes;

- Detecção de intrusão;
- Sistemas de prevenção e combate a incêndio;
- Segurança armada, portaria e guarda de perímetro.

2.5. Governança e Alinhamento Estratégico

Segundo Weill (WEILL e ROSS, 2004) é fundamental a compreensão dos conceitos envolvidos na governança para que seja dado um embasamento no momento da avaliação e adoção de um modelo de governança específico. Tal conceito é também importante na percepção do posicionamento estratégico das organizações.

Não menos importante, o alinhamento estratégico – AE trata do alinhamento dos recursos da organização com as possíveis ameaças e oportunidades relacionadas ao ambiente.

Neste capítulo, são descritos os conceitos de governança corporativa, alinhamento estratégico, governança em TI e, por fim, a governança em Segurança da Informação.

2.5.1. Governança Corporativa

Visando, principalmente, uma forma eficiente e mais segura de estruturar as relações entre mercado financeiro e as empresas, surge a governança corporativa (GRÜN, 2003) (LOPES, 2006). Grün (GRÜN, 2003) considera a boa governança corporativa como sendo um instrumento que deflagra um círculo virtuoso o qual evidencia a transparência nos procedimentos contábeis e administrativos das empresas de capital aberto e que respeita os direitos de acionistas minoritários. Ainda, sendo capaz de ser a base para sustentar essa empresa de maneira institucional. Historicamente (LETHBRIDGE, 1997) identificamos dois modelos clássicos para governança corporativa, desde que surgiu a discussão sobre monitoramento das relações entre acionistas e administradores:

O modelo anglo-saxão

Predominante nos Estado Unidos da América e Reino Unido, o modelo tem como maior fundamento a pulverização do controle acionário e separação da propriedade de gestão. O modelo anglo-saxão é fortemente orientado para o mercado e também

por ele monitorado. Alem do mercado, são utilizados também controles externos para compor a estrutura regulatória de proteção aos acionistas. Podemos destacar a lei *Sarbanes-Oxley* nos Estados Unidos da América e o *City Code* para o Reino Unido. A adoção de padrões contábeis certificados e responsabilização legal dos gestores pelos números apresentados garantem a proteção aos acionistas (ANDRADE e ROSSETTI, 2004).

O modelo nipo germânico

Predominante na Alemanha e Japão, o modelo tem como principal característica o equilíbrio de interesse dos acionistas e *stakeholders* (colaboradores, funcionários, clientes, consumidores, fornecedores, governo e demais), papel limitado do mercado de capitais e gestão coletiva das empresas (CARVALHO, 2004).

São muitas as definições que podem ser encontradas para designar Governança Corporativa. Segundo OECD (OECD, 2010) podemos definir governança corporativa como a estrutura onde os objetivos mensuráveis da organização são determinados, assegurando e protegendo os direitos dos acionistas, colaboradores, clientes, fornecedores e demais interessados. Controlando e monitorando o que chamamos de elementos-chave, garantimos sua efetividade. São eles os elementos-chave:

- Ativos Humanos:

Todas as pessoas, habilidades, plano de carreira, treinamentos e competências;

- Ativos Físicos:

Equipamentos, estabelecimentos comerciais, manutenção, segurança;

- Ativos Financeiros:

Investimentos, fluxo de caixa, ações, dívidas;

- Propriedade Intelectual:

Sistemas da corporação, processos formalmente patenteados, produtos, serviços, registros;

- Ativos de informação e TI:

Sistemas de informação, validade de dados, digitalização de dados, controle de desempenho e rastreabilidade;

- Ativos de Relacionamento:

Imagem da corporação, reputação, parceiros, marcas, unidades de negócio.

Dentre os seis elementos citados, destacamos os “Ativos de Informação e TI” por oferecer as informações necessárias para sustentar a corporação no controle e monitoramento dos ativos. Tal tarefa seria impossível, ou no mínimo difícil, de realizar sem seu auxílio. Essa ajuda é caracterizada por disponibilizar todos os controles, processos, procedimentos e métricas que tem sua origem em TI (LOPES, 2006).

A Figura 10 abaixo mostra um modelo para Governança Corporativa (WEILL e ROSS, 2004).

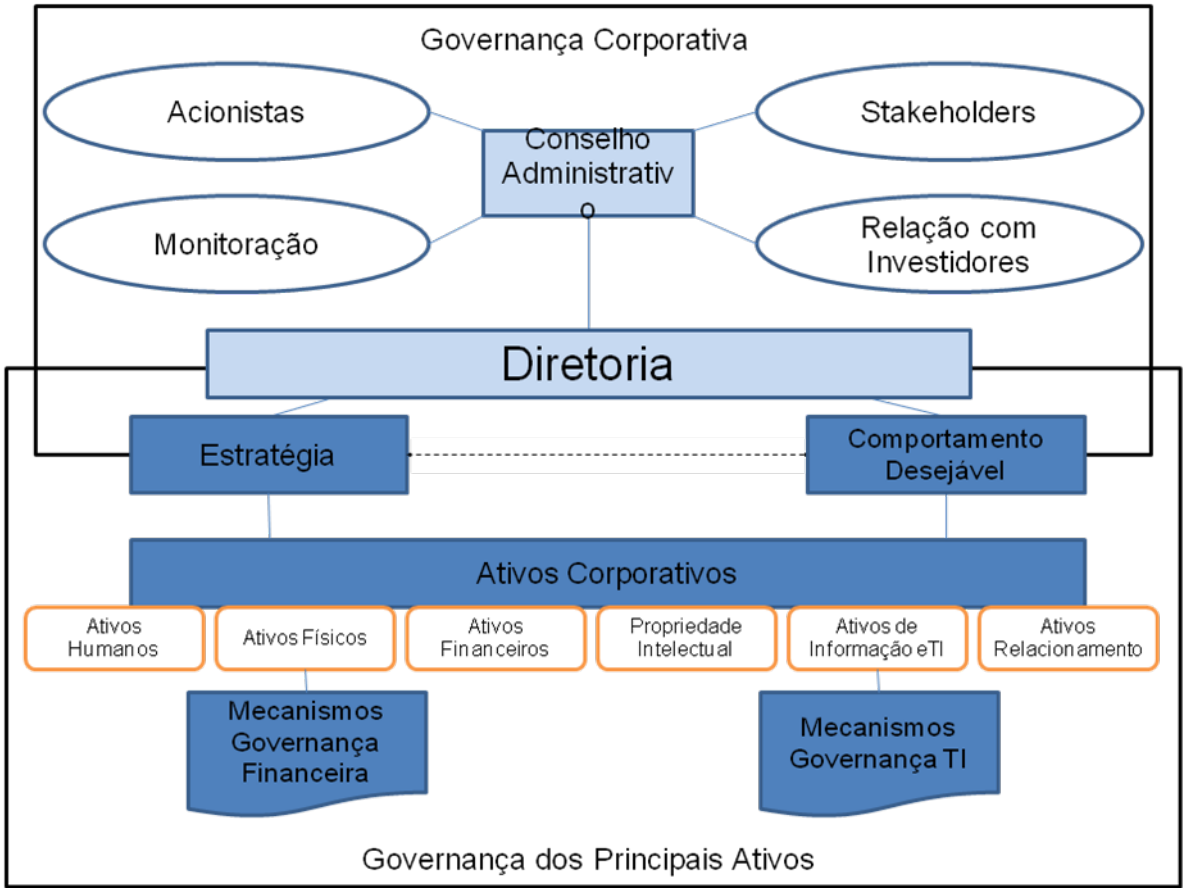


Figura 10: Relacionamento entre Governança Corporativa e Governança de TI

Fonte: (WEILL e ROSS, 2004).

O relacionamento entre diretoria e os demais *players* (acionistas, *stakeholders* e investidores), juntamente com as práticas de monitoramento, são evidenciados na

parte superior do modelo que dessa forma compõe-se a Governança Corporativa. Todas as estratégias e ações para gerar o comportamento desejável, que possibilite que as diretrizes da diretoria sejam alcançadas, são justamente articuladas por seus executivos (membros da Diretoria).

2.5.2. Alinhamento Estratégico

Como mencionado anteriormente, seu conceito reflete a necessidade de alinhamento dos recursos organizacionais com as possíveis ameaças e as oportunidades do ambiente, refletindo as decisões corporativas, as quais alinhadas a seus recursos ajudem na ligação da própria empresa com os componentes de seu ambiente (MILLER, 1998). Um desses recursos corporativos é a própria TI que apoia a estratégia em seu nível operacional ou em níveis mais altos buscando a obtenção de vantagem competitiva (KAPLAN e NORTON, 2004). Esse alinhamento pode ocorrer em diversos níveis de uma organização. No entanto estaremos focados especialmente em dois desses níveis o tático-operacional, onde ocorre a integração funcional entre processos, pessoas do negócio, infraestrutura e suas plataformas tecnológicas e o nível estratégico, no qual ocorre a adequação entre o negócio e TI (TEO e KING, 1997).

A literatura mostra que a partir de 2000, novos modelos complementares e/ou estendidos passam a tratar alinhamento estratégico como um processo contínuo, identificando fatores chamados de habilitadores/inibidores e também o nível de maturidade de AE (LUFTMAN, 2000).

Fatores Habilitadores e Inibidores

Basicamente os fatores habilitadores são aqueles que facilitam de alguma forma o alinhamento estratégico. Já os fatores inibidores exercem um papel contrário, dificultando o alinhamento estratégico entre negócio e TI.

Segundo um estudo realizado por Luftman (LUFTMAN, PAPP e BRIER, 1999) os seguintes fatores habilitadores foram identificados:

- Apoio da alta gestão aos assuntos de TI;
- Envolvimento da TI no desenvolvimento da estratégia;

- Compreensão do negócio por parte da TI;
- Parceria entre TI e área de negócios;
- Projetos de TI corretamente priorizados;
- TI demonstrando liderança.

Ainda, no mesmo estudo, foram apontados como fatores inibidores do alinhamento estratégico do negócio e TI:

- Falta de relacionamento estreito entre TI e área de negócios;
- TI mal priorizada;
- Falha da TI em cumprir seus compromissos;
- Falta de compreensão dos negócios por parte da TI;
- Falta de suporte à TI por parte dos altos executivos;
- Lapso de liderança da gerência de TI.

2.5.3. Governança em TI

Segundo Streit ET AL (STREIT, MAÇADA e BORENSTEIN, 2004), governança de TI está diretamente relacionada com o objetivo de melhorar o desempenho da tecnologia no meio corporativo, adotando melhores práticas, políticas e procedimentos para trabalhar a influência do comportamento empresarial e direcionar as atividades de TI.

A literatura ainda mostra que não somente os profissionais de TI, mas também acadêmicos tem conduzindo pesquisas e também trabalhado no desenvolvimento de teorias e melhores práticas na área (GREMBERGER, 2004). Abaixo alguns conceitos para governança em TI – GTI:

> "Governança de TI é de responsabilidade do Corpo de Diretores e Gerencial. GTI integra a Governança da Empresa e consiste em mecanismos de liderança, estrutura organizacional e processos que garantem que a TI da organização mantém e alcançam as estratégias e objetivos da organização" (ITGI, 2006).
>
> "Governança de TI é a capacidade organizacional exercida pela Diretoria, Gerência Executiva e Gerência de TI para controlar a formulação e implementação da estratégia de TI e neste caminho assegurar a fusão do negócio e TI" (GREMBERGER, 2004).
>
> "Governança de TI é o modelo como as decisões são tomadas e responsabilidades direcionadas para encorajar um comportamento desejável no uso de TI" (WEILL e ROSS, 2004).

Ainda que apresentem diferenças em alguns aspectos, todas as definições acima focam o alinhamento entre negócio e TI. Essa ligação pode ser alcançada através da Governança de TI, sendo parte integrante da Governança Corporativa (ITGI, 2006). A Figura 4 mostra exatamente essa ligação entre Governança Corporativa e GTI. Podemos perceber que TI, sendo de responsabilidade da Diretoria e Gerência Executiva (GREMBERGER, 2004) (ITGI, 2006), é um dos ativos controlados pela Governança Corporativa. Fica claro que GTI é originada a partir da atuação da Governança Corporativa, recebendo o devido alinhamento para a realização de seus projetos. Todas as definições estratégicas são originadas na governança corporativa de modo que suas ações passam a depender de um plano estratégico determinado pela alta gestão.

A forma como a governança corporativa atua estrategicamente dará origem a governança de TI que tem como entrada (*input*) instruções buscando o alinhamento de suas ações como subconjunto da estratégia de negócios (ALBERTIN, 2005).

CobiT

O CobiT - *Control Objectives for Information and Related Technology* – foi desenvolvido pelo ISACA (*Information System Audit and Control Association*) na segunda metade da década de 90 e basicamente permite que a empresa tenha uma visão holística em relação a TI. Sua estrutura tem como base indicadores de desempenho e o monitoramento é realizado com o intuito de quantificar os resultados de TI em relação ao possível valor agregado ao negócio.

Fornece boas práticas através de modelo de domínios e processos e apresenta atividades através de uma estrutura lógica e gerenciável (INSTITUTE, 2007).

O CobiT é ilustrado por um modelo de processos de TI subdivididos em quatro domínios e trinta e quatro processos em linha com as áreas responsáveis por planejar, construir, executar e monitorar (INSTITUTE, 2007). Assim, fornecendo uma visão total dá área de TI. A Figura 11 abaixo mostra uma visão dos quatro domínios do CobiT e suas interações:

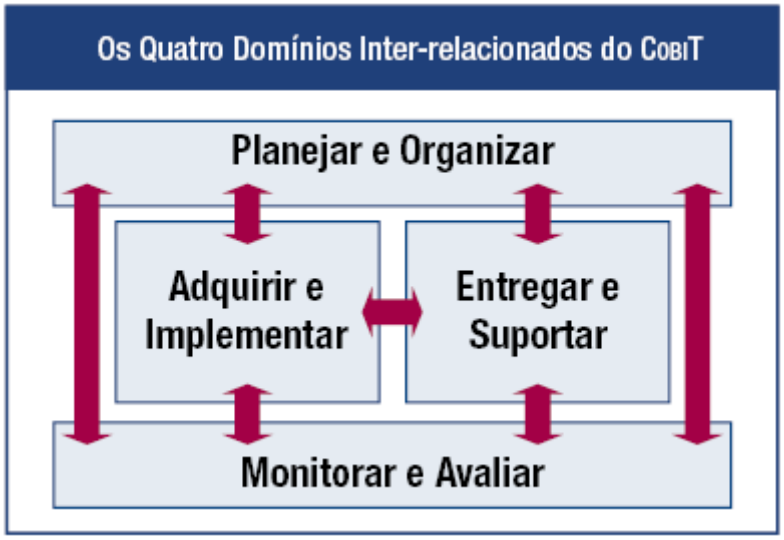


Figura 11: Domínios do CobiT
Fonte: (INSTITUTE, 2007)

Desta forma, segue uma descrição mais detalhada de cada um dos quatro domínios apresentados pelo Cobit:

PLANEJAR E ORGANIZAR (PO)

Domínio responsável por toda a estratégia e as táticas, tendo como principal objetivo identificar como TI deve contribuir para que o negócio alcance seus objetivos. Tipicamente este domínio busca respostas para as seguintes questões gerenciais:

- As estratégias de TI e de negócios estão alinhadas?
- A empresa está obtendo um ótimo uso dos seus recursos?
- Todos na organização entendem os objetivos de TI?
- Os riscos de TI são entendidos e estão sendo gerenciados?
- A qualidade dos sistemas de TI é adequada às necessidades de negócios?

O domínio Planejar e Organizar (PO) está dividido em dez macro controles como segue:

PO1 - Definir um Plano Estratégico de TI
PO2 - Definir a Arquitetura da Informação
PO3 - Determinar as Diretrizes de Tecnologia
PO4 - Definir os Processos, a Organização e os Relacionamentos de TI
PO5 - Gerenciar o Investimento de TI

PO6 - Comunicar Metas e Diretrizes Gerenciais
PO7 - Gerenciar os Recursos Humanos de TI
PO8 - Gerenciar a Qualidade
PO9 - Avaliar e Gerenciar os Riscos de TI
PO10 - Gerenciar Projetos

Desses macro controles vale destacar o controle de número nove – PO9 Avaliar e Gerenciar os Riscos de TI. Este controle tem como principal objetivo a preservação do valor de forma que o gerenciamento de riscos, não importando sua natureza, traga uma transparência para todas as partes envolvidas. O processo em questão deve ser contínuo, com seu início na identificação dos riscos e finalizando sem sua mitigação através da adoção e/ou aplicação de certos controles. Vale lembrar que mesmo após sua mitigação, possivelmente exista o que chamamos de risco residual o qual deve ter sua aceitação declarada pelo corpo executivo da empresa e consequentemente seu gerenciamento, medidas e monitoramento contínuos.
De forma mais detalhada, o controle PO9 - Avaliar e Gerenciar os Riscos de TI é dividido da seguinte forma (INSTITUTE, 2007):

PO9.1 - Alinhamento da gestão de riscos de TI e de Negócios
Estabelecer uma estrutura de gestão de riscos de TI alinhada com a estrutura de gestão de riscos da corporação.

PO9.2 - Estabelecimento do Contexto de Risco
Estabelecer o contexto ao qual a estrutura de avaliação de risco é aplicada para assegurar resultados esperados. Isso inclui a definição dos contextos interno e externo de cada avaliação de risco, o objetivo da avaliação e os critérios pelos quais os riscos são avaliados.

PO9.3 - Identificação de Eventos
Identificar eventos (importante ameaça real que explora significativas vulnerabilidades) com potencial impacto nos objetivos ou nas operações da organização, incluindo aspectos do negócio, regulamentação, aspectos jurídicos, tecnologia, parcerias de negócio, recursos humanos e operacionais. Determinar a

natureza do impacto e manter esta informação. Registrar e manter um histórico dos riscos relevantes.

PO9.4 - Avaliação de Risco

Avaliar regularmente a probabilidade e o impacto de todos os riscos identificados, utilizando métodos qualitativos e quantitativos. A probabilidade e o impacto associado ao risco inerente e residual devem ser determinados individualmente, por categoria e com base no portfólio da organização.

PO9.5 - Resposta ao Risco

Desenvolver e manter um processo de respostas a riscos para assegurar que controles com uma adequada relação custo-benefício mitiguem a exposição aos riscos de forma contínua. O processo de resposta ao risco deve identificar estratégias de risco, tais como evitar, reduzir, compartilhar ou aceitar o risco, determinar responsabilidades, e considerar os níveis de tolerância definidos.

PO9.6 - Manutenção e Monitoramento do Plano de Ação de Risco

Priorizar e planejar as atividades de controle em todos os níveis da organização para implementar as respostas aos riscos identificadas como necessárias, incluindo a identificação de custos, benefícios e responsabilidade pela execução. Obter aprovações para ações recomendadas e aceitação de quaisquer riscos residuais e assegurar que as ações aprovadas sejam assumidas pelos donos dos processos afetados. Monitorar a execução dos planos e reportar qualquer desvio para a Alta Direção.

ADQUIRIR E IMPLEMENTAR (AI)

Para que os objetivos do planejamento estratégico de TI sejam atingidos, todas as soluções necessitam ser identificadas, adquiridas (ou desenvolvidas), implementadas e integradas ao processo de negócios. Todas as alterações e manutenções nos sistemas então existentes também são cobertas por esse domínio. Assim, pode-se garantir que as soluções continuem a atender os objetivos dos negócios. Tipicamente este domínio ajuda a responder as seguintes questões de gerenciamento:

- Os novos projetos fornecerão soluções que atendam às necessidades de negócios?
- Os novos projetos serão entregues no tempo e orçamento previstos?
- Os novos sistemas ocorreram apropriadamente quando implementados?
- As alterações ocorrerão sem afetar as operações de negócios atuais?

ENTREGAR E SUPORTAR (DS)

A entrega dos serviços solicitados, incluindo o gerenciamento da segurança e continuidade, serviços de suporte para usuários e gerenciamento de dados e recursos operacionais, é de responsabilidade deste domínio. Trata geralmente das seguintes questões de gerenciamento:

- Os serviços de TI estão sendo entregues de acordo com as prioridades de negócios?
- Os custos de TI estão otimizados?
- A força de trabalho está habilitada para utilizar os sistemas de TI de maneira produtiva e segura?
- Os aspectos de confidencialidade, integridade e disponibilidade estão sendo contemplados para garantir a segurança da informação?

MONITORAR E AVALIAR (ME)

Para garantir a qualidade e a aderência aos requisitos de controle, este domínio regularmente avalia todos os processos de TI. Abordando questões do gerenciamento de desempenho, monitoramento do controle interno, a aderência regulatória e a governança. Trata geralmente das seguintes questões de gerenciamento:

- O desempenho de TI é mensurado para detectar problemas antes que seja muito tarde?
- O gerenciamento assegura que os controles internos sejam efetivos e eficientes?
- O desempenho da TI pode ser associado aos objetivos de negócio?

- Existem controles adequados para garantir confidencialidade, integridade e disponibilidade das informações?

A Figura 12 abaixo mostra uma visão geral dos domínios acima e seus controles:

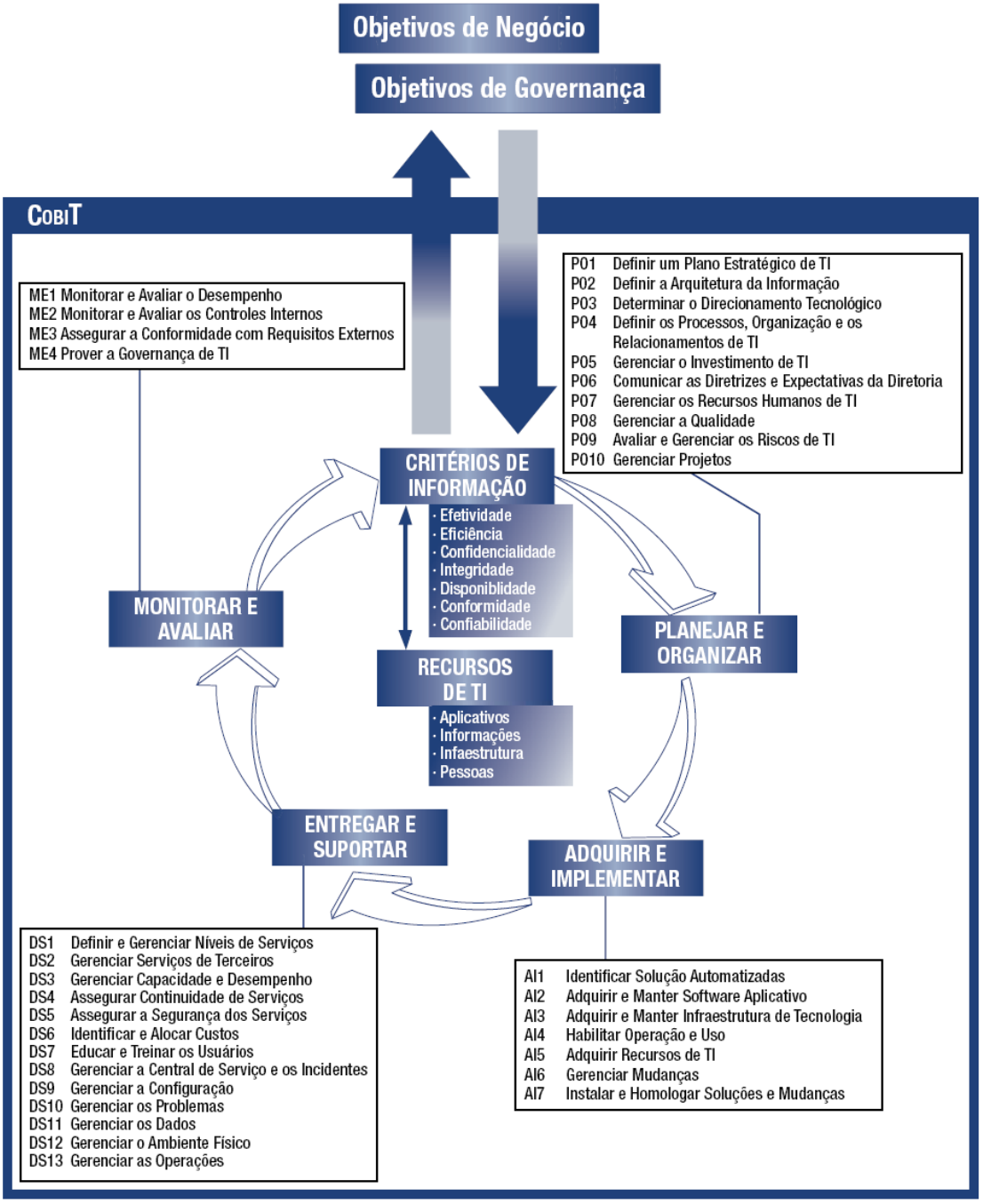


Figura 12: Visão geral do modelo CobiT

Fonte: (INSTITUTE, 2007)

ITIL

Information Technology Infrastructure Library – ITIL é uma estrutura (*framework*) que descreve as melhores práticas para gerenciamento de serviços de TI. Com foco no

monitoramento e melhoria na qualidade de entrega dos serviços prestados por TI pelas diferentes perspectivas do usuário e negócio (FORUM, 2007). Alguns dos benefícios alcançados através da prática do ITIL:

- Aumento da satisfação por parte do usuário com os serviços de TI;
- Melhoria da disponibilidade do serviço, o que está diretamente ligado ao aumento de receita;
- Redução de retrabalho, tempo médio gasto e melhoria no uso e gerenciamento de recursos;
- Melhoria na tomada de decisão.

Inicialmente publicado na década de 1980 pelo governo britânico, hoje conhecido como *Office of Government Commerce – OGC,* e reconhecido mundialmente como padrão ou modelo na década de 1990, teve sua versão inicial revisada nos anos entre 2000 e 2004. Em sua primeira edição continha trinta e um livros os quais cobriam todos os aspectos da provisão de serviços em TI. Já em sua segunda versão, todos esses aspectos foram resumidos em apenas sete livros que passou a se chamar ITIL V2 consolidando assim o *framework*.

Em sua versão mais recente, ITIL V3 mostrado na Figura 13, o *framework* foi consolidado e melhorado em apenas cinco livros principais – Ciclo de Vida de Serviços, Estratégia de Serviço, Design de Serviço, Transição de Serviço e Operação de Serviços – todos cobrindo cada estágio desse ciclo, mostrado em maiores detalhes na Figura 14 - Estágios do ciclo de vida de Serviços e suas ligações.

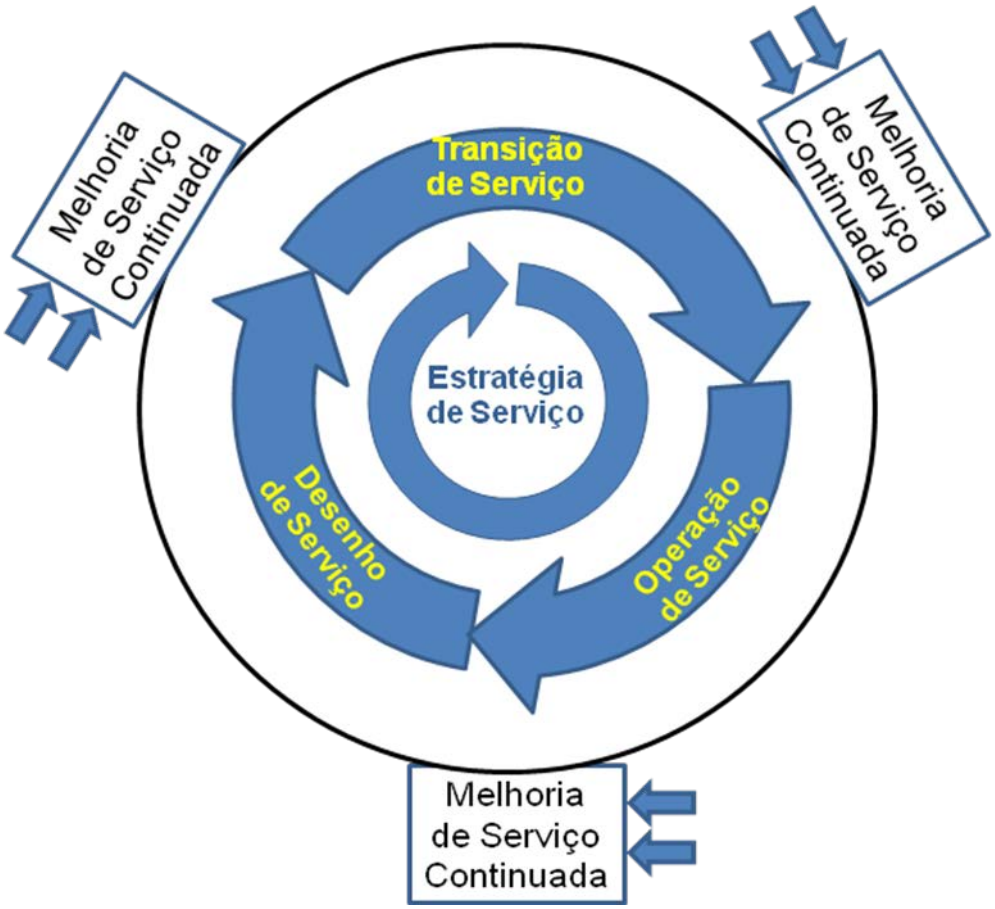


Figura 13: Ciclo de vida do ITIL
Fonte: Adaptação de (FORUM, 2007)

Todas as soluções e atividades relacionadas a serviços devem ser direcionadas através das necessidades e requerimentos do negócio. Essas ações deverão refletir a estratégia e políticas da corporação. A Figura 14 ilustra como o ciclo de vida é iniciado através da necessidade do negócio. Essas necessidades devem ser identificadas e alinhadas com a Estratégia de Serviços definindo o conjunto de entregáveis. Esses passam através do Design de Serviço onde a solução é propriamente desenvolvida contendo tudo que é necessário para levar o serviço através dos demais estágios.

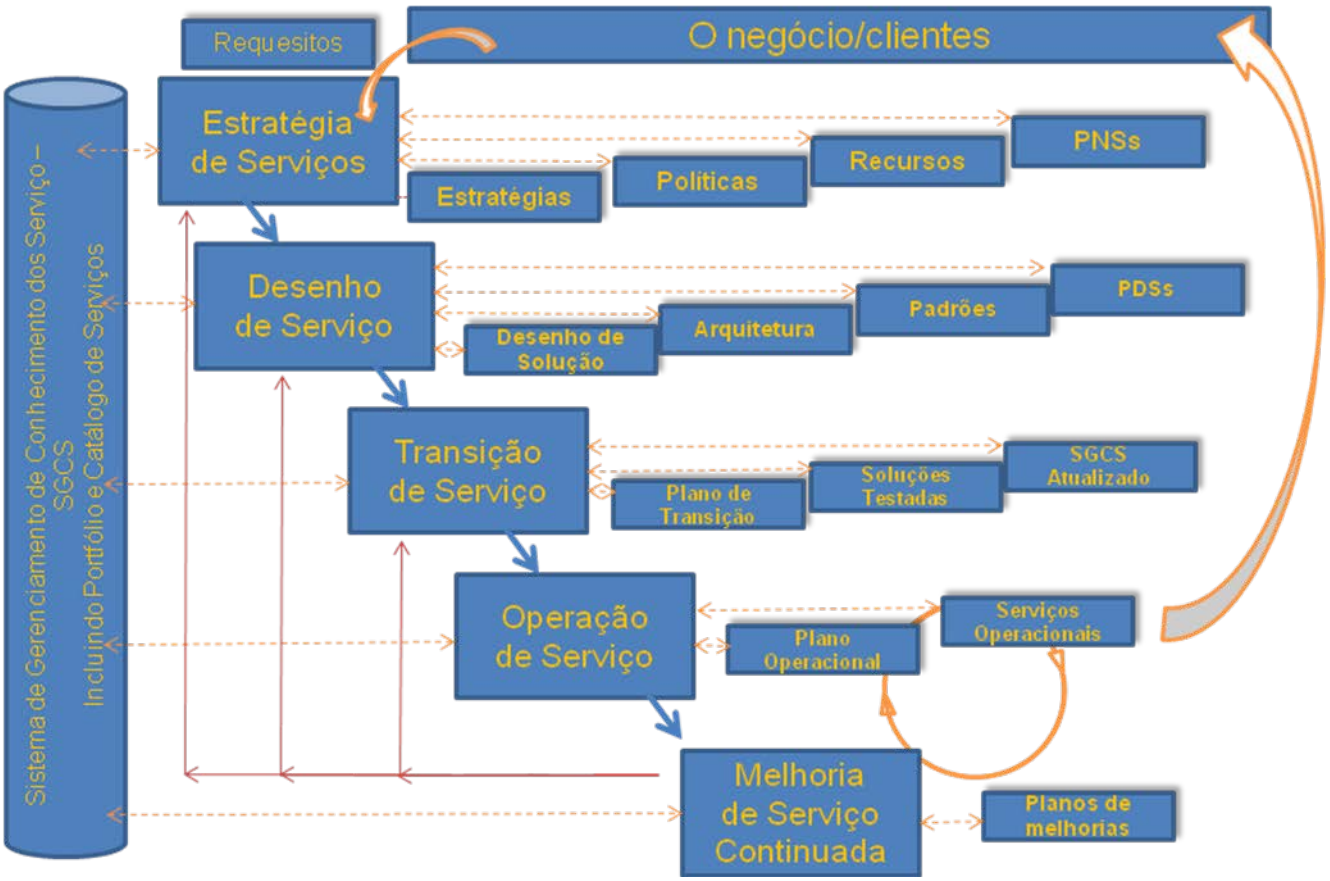


Figura 14: Estágios do ciclo de vida de Serviços e suas ligações

Fonte: Adaptação de (FORUM, 2007)

Estratégia de Serviço

A Estratégia de Serviço tem como base o ciclo de vida do *ITIL V3.* Fornece o norte para os provedores de serviço em TI e seus clientes, ajudando os mesmos a operar e prover seus serviços com qualidade. Também a priorizar investimentos sobre o provimento de serviços. Para isso, é fundamental o verdadeiro entendimento de (FORUM, 2007):

- Qual serviço deve ser ofertado;
- A quem esse serviço deve ser ofertado;
- Melhor entendimento dos mercados interno e externo;
- Como criar o real valor de um serviço a partir da percepção do cliente e acionista;
- Como seu desempenho será medido.

A literatura ainda nos mostra alguns conceitos chave para a Estratégia de Serviço. Esses conhecidos como os quatro P's, onde juntos formam a estratégia:

✓ **Perspectiva**

Visão da Organização onde se define seus valores e convicções. Direção no qual provedor de serviço vai alcançar seus objetivos.

✓ **Posição**

Define qual é a imagem que a organização vai ter para seus clientes. Quais os serviços serão ofertados no mercado.

✓ **Plano**

Tornar-se competitiva. Melhor detalhamento da execução de sua estratégia.

✓ **Padrão**

Fundamentalmente representa a forma de como executar tudo. São colocados em forma de procedimentos de uma organização. Como resultado da perspectiva, posição e plano surgem os padrões.

Figura 15: Os quatro P's da Estratégia de Serviço.
Fonte: O autor.

Design de Serviço

Parte integrante do ciclo de vida do *ITIL V3* é um elemento importante no processo de mudança de negócio. A literatura define como principal papel do Design de Serviço como sendo (FORUM, 2007):

> "O design inovador e apropriado do serviço de TI, incluindo sua arquitetura, processos, políticas e documentação, para satisfazer os requerimentos acordados atuais e futuros do negócio."

Fornece guia para a criação e manutenção de políticas de TI, arquiteturas e documentos para o desenho de apropriadas e inovadoras infraestruturas de solução de serviços e processos de TI. Provê também uma abordagem para o Desenho de Serviços novos ou alterados para a transição para o ambiente de produção.
O Design de Serviços busca contemplar o desenvolvimento de serviços satisfazendo o alinhamento com os objetivos do negócio, dentro de uma escala de tempo e custo. Visa processos eficientes e eficazes na gerência de serviços durante todo seu ciclo de vida. Incluindo todos os processos de transição e manutenção daquele serviço em operação.
Não podendo deixar de lado a identificação e gerência de riscos. Alguns deles já assumidos ainda na fase da estratégia. O Design de Serviços busca estruturas seguras e tolerantes a falhas.
Os princípios que mais se destacam no Design de Serviços são:

- ✓ **Identificação dos requisitos de negócio, definição dos requisitos do serviço e desenho do Serviço**
  - Contemplando os requisitos das novas funcionalidades ou mudanças do serviço;
- ✓ **Portfólio de Serviços**
  - Contém detalhes de todos os serviços e seus status
- ✓ **Desenho da Arquitetura e Tecnologia**
  - O desenho de processos necessários para transição, operação e melhoria continuada. Para todo processo é necessário um proprietário, responsável pelo seu aperfeiçoamento e pela garantia que ele atenda seus objetivos;

- ✓ **Desenho do processo**

- Desenho de processos necessários para transição, operação e melhoria continuada;

✓ **Desenho de Métricas e medição**

- Não havendo a possibilidade de medição, o gerenciamento poderá ficar comprometido. Portanto, a necessidade de estabelecer métricas é de suma importância para todos os processos;
- Essas métricas devem garantir a verificação do nível de qualidade e propósito de cada serviço.

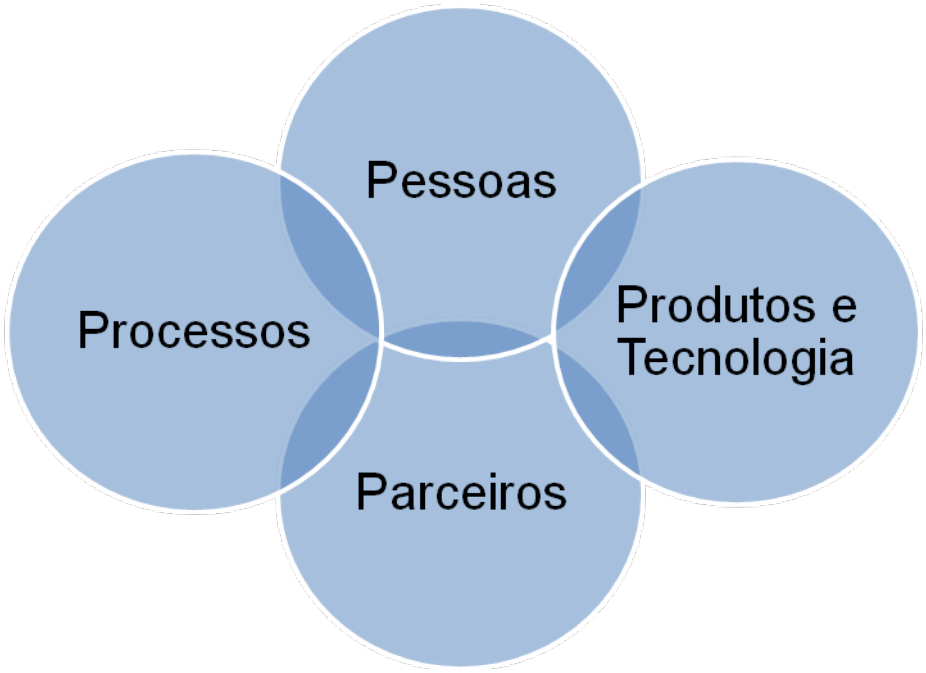


Figura 16: Os quatro P's do Design de Serviço.
Fonte: O autor

A Figura 16 detalha uma visão mais holística adotada pelo Design de Serviço onde é necessário determinar os papéis das pessoas em cada processo a ser definido. Determinar produtos, serviços, tecnologia e ferramentas. E por fim, estabelecer seus parceiros formando assim os quatro P's para Design de Serviço.

Ainda em Design de Serviço devemos dar destaque ao sistema de gestão de segurança da informação através da definição de processos que garantem a confidencialidade, integridade e disponibilidade dos ativos da organização, da própria informação, de dados e serviços de TI.

Segurança da informação tem um capítulo, no livro Design de Serviço, completo dedicado ao seu sistema de gestão, Sistema de Gestão de Segurança da Informação – SGSI onde um *framework* é apresentado para o desenvolvimento de um programa de segurança, que tenha um bom custo-benefício, de forma a fornecer suporte aos objetivos do negócio. Esse *framework:* controlar, planejar, implementar, avaliar e manter, que é utilizado para gerenciar segurança em TI é descrito em maior detalhe como segue:

Controlar

Os objetivos dos elementos de controle do SGSI são para:

- Estabelecer uma estrutura de gerenciamento para iniciar e gerenciar segurança da informação dentro da organização.
- Estabelecer uma estrutura organizacional para preparar, aprovar e implementar uma Política de Segurança da Informação.
- Definir responsabilidades.
- Estabelecer e controlar documentação.

Planejar

O principal objetivo dessa fase do *framework* é criar e recomendar medidas de segurança apropriadas, baseadas no bom entendimento dos requisitos do negócio.

Esses requisitos devem ser entendidos a partir de fontes como o próprio negócio, gerenciamento de risco, planos e estratégias, acordo de níveis de serviço (SLAs) e responsabilidades legal, moral e ética para a segurança da informação.

A Política de Segurança da Informação define a postura da organização para os assuntos de segurança. Esta deve ser um documento corporativo, ao alcance de todos e não somente aplicada à serviços de TI.

Implementar

O objetivo de implantar o SGSI é garantir que os procedimentos, ferramental e controles apropriados estão adequadamente alinhados com a Política de Segurança da Informação como, por exemplo:

- Responsabilidade de ativos – Gerenciamento de configuração e Sistema de gerenciamento de configuração tem um papel fundamental para uma implementação de sucesso do SGSI.
- Classificação da informação – Informação e seus repositórios devem ser classificados de acordo com a sensibilidade e impacto de sua divulgação.

Outros fatores são fundamentais para uma implementar os controles e medidas de segurança como sucesso:

- Uma Política clara e que possua o apoio da alta gestão, integrada com a necessidade do negócio.
- Procedimentos de segurança que sejam devidamente justificados, apropriados e também apoiados pela alta gestão corporativa.
- Treinamento e conscientização apropriados em requisites de segurança.
- Mecanismo de melhoria.

Avaliar

Os objetivos do elemento avaliação do SGSI são:

- Supervisionar e checar a conformidade com a Política de Segurança da Informação e seus requisites em relação a acordo de níveis de serviço e operação (SLAs e OLAs).
- Auditoria interna de segurança para sistemas de TI.
- Prover informação para auditorias externas e/ou regulamentações, quando necessário.

Manter

Os objetivos desse elemento do SGSI são:

- Melhoria de acordos de segurança especificados em, por exemplo, SLAs e OLAs.

- Melhoria na implementação de medidas e controles de segurança.

Para que isso seja alcançado o ciclo PDCA deverá ser utilizado, através de formalização sugerida pela ISO IEC 27001.

Transição de Serviço

O principal papel da Transição de Serviço é a entrega do serviço requerido pelo negócio em modo operacional (FORUM, 2007). Isso acontece quando Transição de Serviço recebe o Pacote de Design de Serviço – PDS proveniente do estágio mencionado acima, o Design de Serviço. De forma que todo e qualquer elemento necessário para sua operação e suporte de um determinado serviço seja entregue.

O estágio Transição de Serviço se preocupa com a implementação de todos os aspectos de um determinado serviço, não somente quando utilizado em condições normais, mas é necessário também garantir que o mesmo possa operar em circunstâncias adversas, provendo suporte para possíveis falhas e erros.

Transição de Serviço busca suporte em princípios que facilitam a efetividade e eficácia do uso de um novo e/ou serviço modificado. Podemos citar como princípios:

- Entendimento de todos os serviços, suas utilidades e garantias;
- Estabelecimento de políticas formais e *framework* padrão para a implementação de todas as mudanças requeridas;
- Suporte a transferência de conhecimento, suporte a decisão e a reutilização de processos, sistemas e outros elementos;
- Antecipar e gerenciar as possíveis mudanças de curso;
- Garantir o envolvimento Transição de Serviço e seus requerimentos através do ciclo de vida de Serviço.

Um conjunto de três processos – Gerenciamento de Mudança, Gerenciamento de Configuração e Ativo de Serviço e Base de Conhecimento – se destaca em Transição de Serviço por tratar de processos que possui impacto, entrada/monitoramento e controle por todos os estágios do ciclo de vida.

✓ **Gerenciamento de Mudança**

O Gerenciamento de Mudança deve garantir que toda e qualquer mudança seja documentada, avaliada, autorizada, priorizada, planejada, testada, implementada e revista de forma controlada. O principal objetivo do processo de Gerenciamento de

Mudança é garantir que métodos padronizados sejam utilizados para a eficiência de todas as mudanças, garantir também que todas as mudanças sejam devidamente documentadas em um sistema de gerenciamento de configuração e por fim, que os riscos inerentes a mudança sejam identificados e mitigados.

> "Gerenciamento de Mudança é a adição, modificação ou remoção de um serviço ou componente de serviço autorizado, planejado ou suportado e sua documentação associada." (FORUM, 2007)

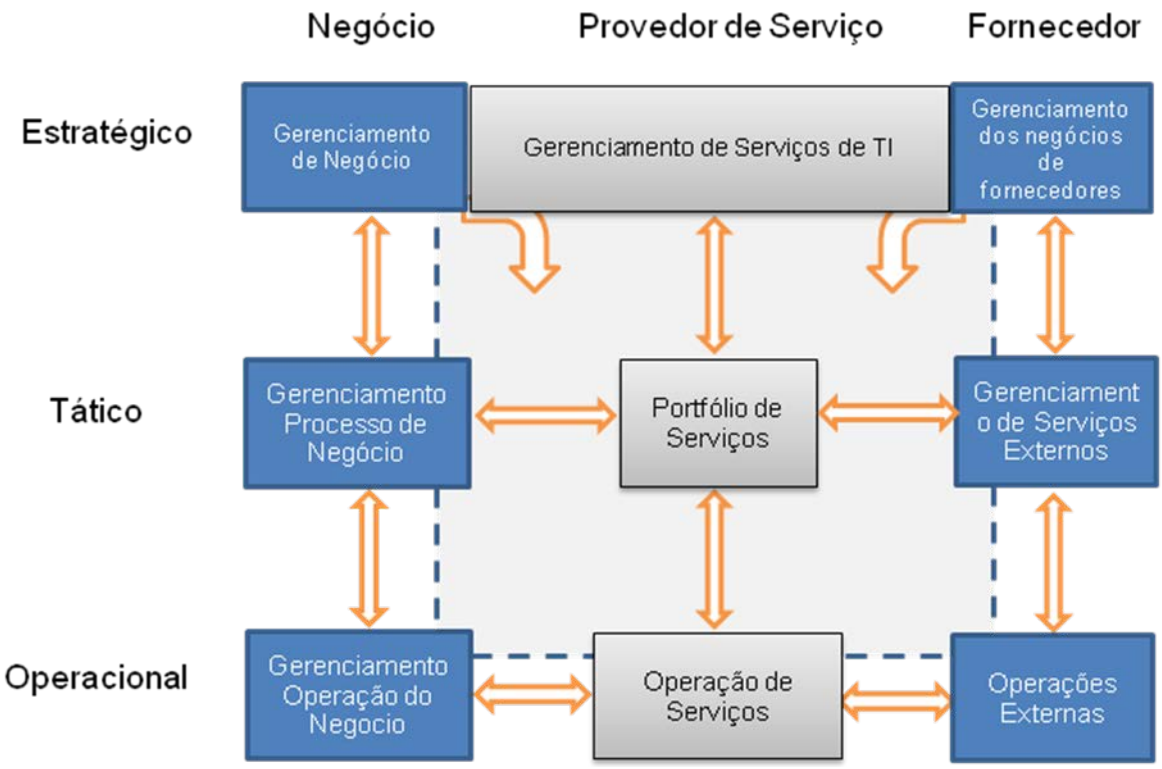


Figura 17: Ciclo de vida Gerenciamento de Mudança
Fonte: Adaptação de (FORUM, 2007)

A Figura 17 detalha a relevância do Gerenciamento de Mudança por todo o ciclo de vida, sendo aplicado em todos os níveis – Estratégico, Tático e Operacional – de gerenciamento de serviço.

✓ **Gerenciamento de Configuração e Ativo de Serviço - GCAS**

O GCAS tem como principal objetivo apoiar o negócio provendo informações e controles precisos sobre todos os ativos, e seus relacionamentos, de infraestrutura

corporativa. Fundamentalmente o GCAS identifica, controla e mantém todos os itens de configuração (IC) pertinentes aos serviços corporativos ofertados por TI, protegendo e garantindo sua integridade ao longo de todo o ciclo de vida do serviço.
A abrangência de atuação do GCAS vai além do controle de os itens de configuração internos. São controlados também aqueles ativos que chamamos de externos ou que são compartilhados por estruturas compartilhadas. Para o gerenciamento de grande e complexo portfólio de serviços e ativos de infraestrutura, é recomendada a utilização de um Sistema de Gerenciamento de Configuração (SGC).

- ✓ **Base de Conhecimento**

O gerenciamento do conhecimento tem como propósito garantir que a pessoa correta tenha o conhecimento correto no momento necessário para que o suporte aos serviços seja entregue com qualidade de acordo com a necessidade do negócio. Desta forma contribuindo para que:

- ✓ Serviços com maior qualidade e eficiência
- ✓ Claro entendimento do valor prestado pelos serviços
- ✓ Que a informação relevante esteja sempre disponível

Em outras palavras, aquela estrutura de dados, informações e conhecimentos sem tratamento é transformada em ativo importante para a prestação de serviços dentro da corporação.

Operação de Serviço

A operação de serviço tem como propósito as entregas acordadas (*Service Level Agreement - SLAs)* de todos os serviços oferecidos por TI para seus usuários e clientes, gerenciar aplicações, tecnologia e toda infraestrutura que apoia tais entregas.
Assim como os estágios, mostrado na Figura 8, do ciclo de vida de Serviços, nesse estágio destacamos os seguintes principais processos:

- ✓ **Gerenciamento de Eventos**

Definimos evento como qualquer mudança de estado que tenha significância para o Gerenciamento de Configuração ou para qualquer serviço de TI (FORUM, 2007).

- ✓ **Gerenciamento de Incidentes**

Qualquer interrupção não planejada para um serviço de TI ou qualquer redução na qualidade desse serviço ofertado é considerada como sendo um incidente. Também consideramos como incidente qualquer falha de um item de configuração que ainda não tenha impactado algum serviço de TI (FORUM, 2007).

- ✓ **Gerenciamento do Cumprimento de Solicitações**

Uma requisição de serviço é qualquer requisição de um usuário e/ou cliente em busca de informação/suporte, mudança padrão ou acesso à um serviço de TI.

O propósito do gerenciamento do cumprimento de solicitações é garantir que o usuário e/ou cliente tenha plenas condições de solicitação e recebimento de serviços padrão ofertados por TI, entrega desses serviços, provimento de informações sobre serviços e procedimentos de como obtê-los e assistir com as possíveis reclamações e comentários dos usuários e/ou clientes.

- ✓ **Gerenciamento de Problemas**

Podemos dizer que um problema é a causa de um ou mais incidentes. Geralmente não se conhece a causa do problema no momento em que o mesmo é gerado e sua investigação é de responsabilidade do gerenciamento de problemas.

O gerenciamento de problemas tem como principal objetivo prevenir problemas, eliminar a reincidência de incidentes e minimizar qualquer que seja o impacto para o usuário e/ou cliente.

- ✓ **Gerenciamento de Acessos**

O principal propósito do gerenciamento de acessos é garantir que cada usuário/cliente tenha o direito de acesso ao serviço ou um grupo de serviços de forma que qualquer acesso não autorizado seja evitado. Gerenciando diretamente a confidencialidade, disponibilidade e integridade das informações corporativas e também sua propriedade intelectual.

Melhora Contínua de Serviço

O propósito da melhora continua de serviço é garantir que a percepção do valor do serviço para o usuário e/ou cliente seja mantido, ou melhorado, através de avaliações contínuas e melhoria da qualidade dos serviços de TI. A Figura 18 mostra

o modelo de como se identificar e gerenciar as melhorias necessárias comparando a situação atual de um determinado serviço e qual seu real valor para o negócio, com os objetivos em longo prazo identificando assim possíveis falhas.

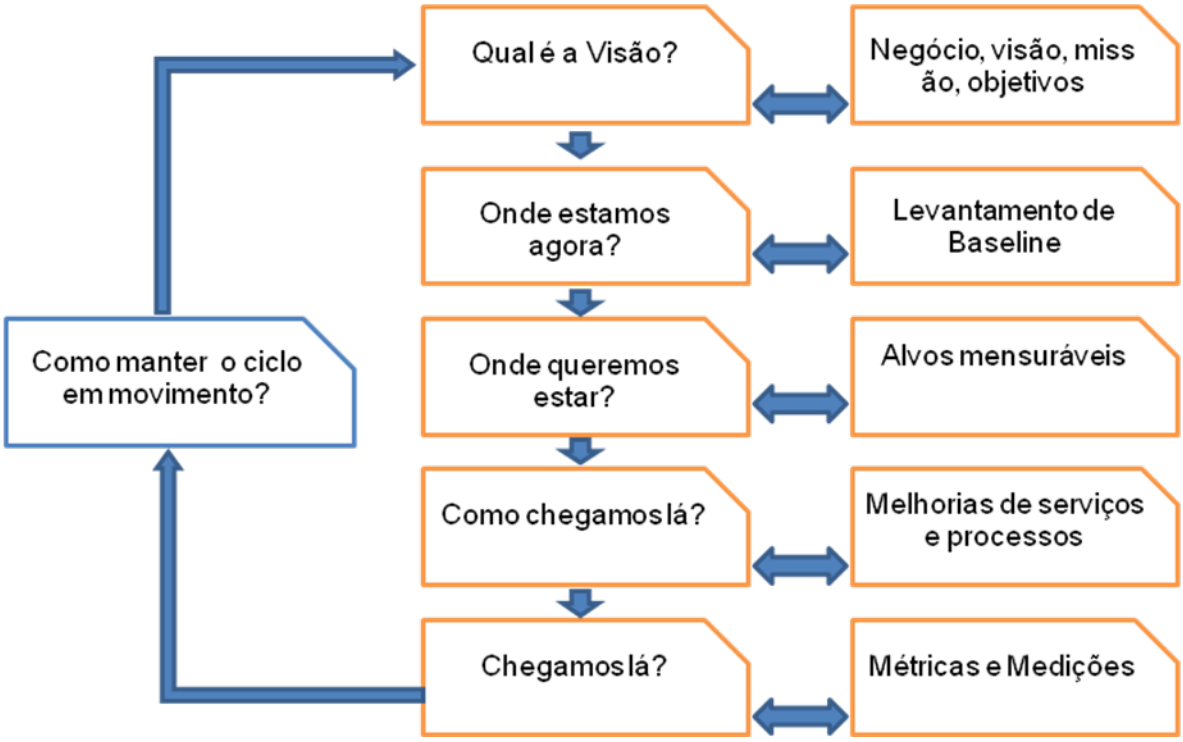


Figura 18: Modelo de Melhora Contínua de Serviço

Fonte: Adaptação de (FORUM, 2007)

Para que a melhora contínua de serviço possua uma implementação efetiva, três processos são definidos: Processo de melhoria dos 7-passos, Medição de serviço e Relatório de serviço.

3. Taxonomia proposta para riscos operacionais relacionados à Segurança da Informação para o mercado segurador

Ainda observando a literatura, item 2.2.4, o risco operacional está diretamente relacionado com a execução dos processos de negócio da corporação. Está relacionado a possíveis perdas como resultado de sistemas e/ou controles inadequados, falhas de gerenciamento e erros humanos (DUARTE JR., 1996).

O capítulo destina-se ao detalhamento de uma proposta de classificação de riscos operacionais e sua disposição em uma estrutura taxonômica para empresas do mercado segurador brasileiro sob a visão da segurança da informação.

Para facilitar o entendimento da disposição a ser apresentada pela pesquisa, foi adotada uma nomenclatura própria baseada no conceito de árvore utilizado em estruturas de dados. Partindo de uma raiz, a estrutura ramifica-se em outras estruturas menores denominadas nós. Esses nós podem ser divididos em diversos níveis sem um limite pré-determinado. Para aquele elemento que não possui nenhum nó descendente, a denominação é de folha ou nó-terminal.

Na literatura encontramos uma variedade de definições de risco bem como diversas classificações. No entanto, a pesquisa esta baseada na classificação segundo (DUARTE JR., 1996), que desdobra risco (raiz) em quatro dimensões (nós): risco de mercado, risco de crédito, risco legal e risco operacional conforme Figura 19 abaixo:

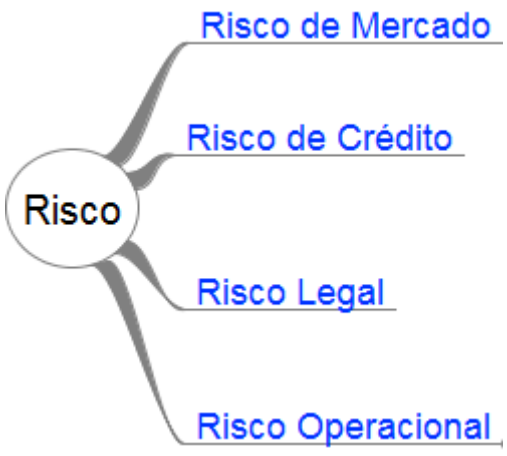


Figura 19: Dimensões de risco
Fonte: O autor

Continuando o desdobramento da estrutura taxonômica, seguimos com o detalhamento para o nó denominado risco operacional, que se divide em três grandes subgrupos: risco organizacional, risco de operações e risco de pessoal conforme mostrado na Figura 20 abaixo.

Figura 20: Classificação risco operacional
Fonte: Autor

3.1. Risco Organizacional

Já mencionado no item 2.1.4-a, o risco organizacional relaciona-se com aquela organização ineficiente, que apresenta deficiência em seus controles internos bem como fraudes, inexistência/deficiência em seus fluxos de informações entre outros (DUARTE JR., 1996).

O risco organizacional divide-se em quatro principais categorias: Fuga de Informação Sensível, Fraudes Internas, Regulamentação e Imagem Corporativa.

3.2. Risco de Operações

O risco de operações é dado pela perda decorrente de qualquer deficiência dos sistemas de informação, como por exemplo, telefonia e computacional. Deficiência no processamento e armazenamento de dados (DUARTE JR., 1996).

3.3. Risco de Pessoal

O risco de pessoal é definido pelas perdas ocasionadas por desvio de conduta de colaboradores seja por mão de obra não qualificada, ambição, insatisfação, desmotivação ou até mesmo comodidade (zona de conforto).

Buscando o desdobramento da primeira folha, risco organizacional, mostramos o detalhamento desse risco conforme mostrado na Figura 21 abaixo:

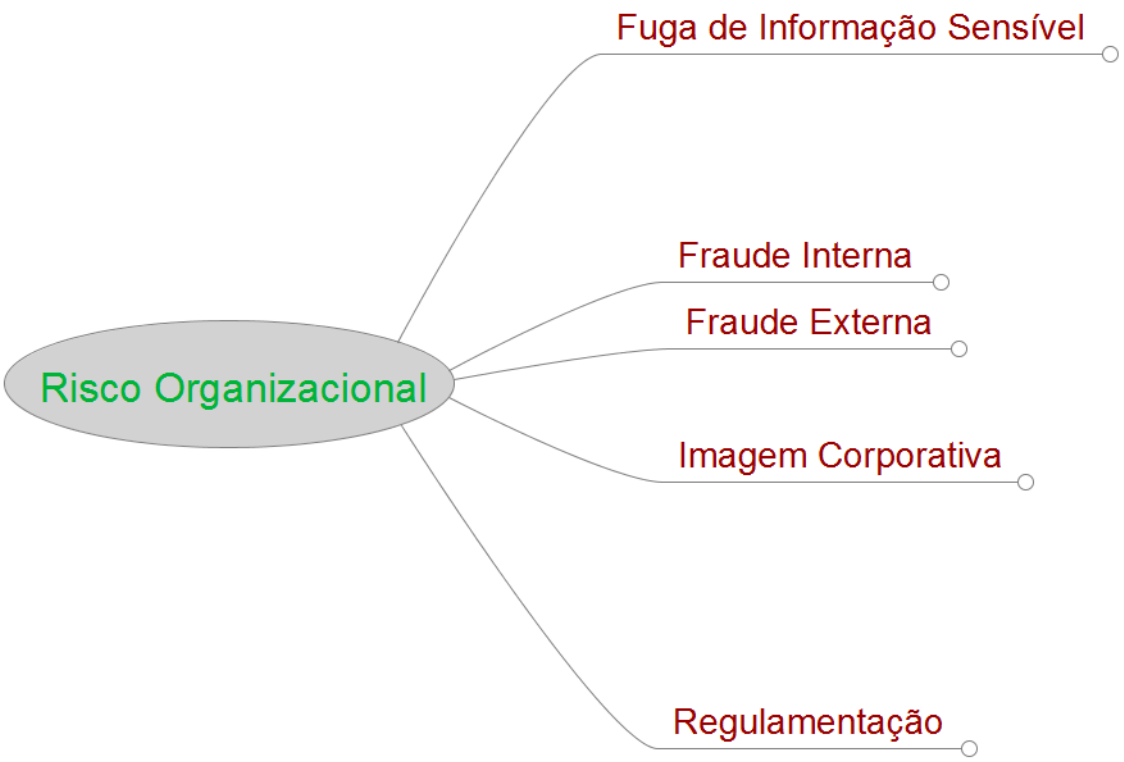


Figura 21: Desdobramento da folha risco organizacional

Fonte: O autor

Onde os nós fuga de informação sensível, fraude interna, fraude externa, imagem corporativa e regulamentação são descritos como segue:

3.4. Fuga de Informação Sensível

Incidentes de fuga de informações vêm ganhando enorme destaque no mercado e imprensa. Alterações no código civil de alguns estados dos Estados Unidos da América tem realizado um papel fundamental para que diversas empresas divulguem tais incidentes. O grande ganho para segurança da informação com tais relatórios de incidentes de fuga de informação sensível são as possibilidades de análise sob nossa ótica a fim de buscar suas causas e consequentemente trabalhar na melhoria dos processos que os envolve minimizando riscos.

Basicamente, para que o risco de fuga de informação sensível se concretize duas etapas devem ser alcançadas: Acesso a informação e o envio para fora dos domínios da corporação.

3.5. Fraude Interna

O risco de fraude interna é definido pela perda em decorrência de comportamento fraudulento (descumprimento intencional de políticas e normas de segurança da corporação, adulteração de controles, etc.) por parte de colaboradores. Assim, trabalhando na obtenção de informação privilegiada para ganho de acesso a um serviço, infraestrutura e/ou informação estratégica.

3.6. Fraude Externa

O risco de fraude externa é definido pela perda em decorrência de comportamento fraudulento, ou seja, descumprimento intencional de políticas e normas de segurança da corporação, adulteração de controles, etc. por parte de terceiros. Assim, trabalhando na obtenção de informação privilegiada para ganho de acesso a um serviço, infraestrutura e/ou informação estratégica.

3.7. Imagem Corporativa

O risco de imagem corporativa decorre das perdas por qualquer que seja a alteração da reputação da corporação diante de seus clientes, parceiros, órgãos públicos e privados, etc.

3.8. Regulamentação

Definimos o risco de regulamentação pela perda em decorrência pela não conformidade com normas para os controles internos bem como as regulamentações do setor.

Continuando seu desdobramento, os nós: fuga de informação sensível, fraude interna, fraude externa, imagem corporativa e regulamentação, são subdivididos conforme segue:

Fuga de Informação Sensível

- Acesso Físico
  - Deficiência de controle
  - Descumprimento de normas internas
- Acesso Lógico
  - Deficiência de controle
  - Descumprimento de normas internas
- Outros

Fraude Interna

- Adulteração de controles
- Descumprimento de normas internas
- Desvio de valores monetários

Fraude Externa

- Seguradoras
  - Adulteração documentos
  - Falsificação documentos
  - Extorsão
- Clientes
  - Adulteração documentos
  - Falsificação documentos
  - Extorsão
- Corretores

    - Adulteração documentos
    - Falsificação documentos
    - Extorsão
- Parceiros
    - Adulteração documentos
    - Falsificação documentos
    - Extorsão
- Outros
    - Adulteração documentos
    - Falsificação documentos
    - Extorsão

Imagem Corporativa

- Divulgação informações
    - Informação imprecisa
    - Informação incompleta
    - Informação incorreta
- Publicidade e Propaganda
    - Informação imprecisa
    - Informação incompleta
    - Informação incorreta
- Comunicação Interna
    - Informação imprecisa
    - Informação incompleta
    - Informação incorreta

Regulamentação

- Normas Internas
    - Inobservância
    - Violação
    - Interpretação indevida
- Normas Externas
    - SUSEP
        - Inobservância

        - Violação
        - Interpretação indevida
    - ANS
        - Inobservância
        - Violação
        - Interpretação indevida
    - Outros
        - Inobservância
        - Violação
        - Interpretação indevida

Buscando o desdobramento do segundo nó, risco de operações, mostramos o detalhamento desse risco conforme mostrado na Figura 22 abaixo:

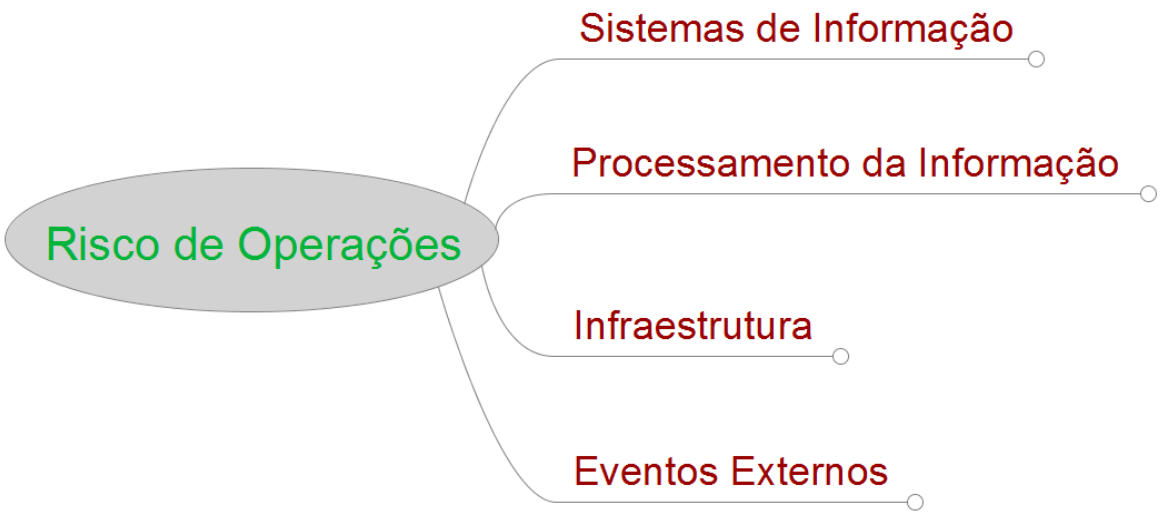


Figura 22: Desdobramento da folha risco de operações
Fonte: O autor.

Onde sistemas de informação, processamento da informação, infraestrutura e eventos externos são descritos como segue:

3.9. Sistemas de Informação

O risco de sistemas de informação caracteriza-se pela perda decorrente da deficiência e/ou falha de qualquer parte integrante do mesmo, seja em telecomunicações, ambiente computacional e/ou outros.

3.10. Processamento da Informação

O risco de processamento da informação é definido pelas perdas causadas por deficiências no processamento de qualquer informação corporativa em tempo hábil e de forma confiável. Esse processamento pode ser descrito como sendo o recebimento, envio e/ou armazenamento da informação.

3.11. Infraestrutura

O risco de infraestrutura é caracterizado pelas perdas causadas em função do comprometimento de qualquer ativo de informação seja ele físico ou lógico.

3.12. Eventos Externos

O risco dado por eventos externos é definido pelas perdas decorrentes de qualquer ação onde o homem não possui controle como, por exemplo, tempestades ou epidemias.

Continuando seu desdobramento, os nós: sistemas de informação, processamento da informação, infraestrutura e eventos externos, são subdivididos conforme segue:

Sistemas de Informação

- Telecomunicações
    - Mau funcionamento
    - Sobrecarga
    - Segurança de ativos
- Computacional
    - Desenvolvimento de Sistemas/Aplicações
    - Segurança de Aplicações
    - Segurança de Ativos
- Outros

- Mau funcionamento
- Sobrecarga
- Segurança de ativos

Processamento da Informação

- Disponibilidade
- Integridade
- Confidencialidade
- Autenticidade
- Processos
  - Faturamento
  - Seguros Gerais
    - Regulação de Sinistro
      - Inadequação da concepção
      - Falta de manutenção/controle
      - Falha comunicação interna
    - Aceitação de Proposta
      - Inadequação da concepção
      - Falta de manutenção/controle
      - Falha comunicação interna
    - Emissão de Apólice
      - Inadequação da concepção
      - Falta de manutenção/controle
      - Falha comunicação interna
    - Outros
  - Seguros Saúde
    - Regulação de Sinistro
      - Inadequação da concepção
      - Falta de manutenção/controle
      - Falha comunicação interna
    - Aceitação de Proposta
      - Inadequação da concepção
      - Falta de manutenção/controle

        - Falha comunicação interna
    - Emissão de Apólice
        - Inadequação da concepção
        - Falta de manutenção/controle
        - Falha comunicação interna
    - Outros

- Seguros Pessoas
    - Regulação de Sinistro
        - Inadequação da concepção
        - Falta de manutenção/controle
        - Falha comunicação interna
    - Aceitação de Proposta
        - Inadequação da concepção
        - Falta de manutenção/controle
        - Falha comunicação interna
    - Emissão de Apólice
        - Inadequação da concepção
        - Falta de manutenção/controle
        - Falha comunicação interna
    - Outros
- Capitalização
    - Regulação de Sinistro
        - Inadequação da concepção
        - Falta de manutenção/controle
        - Falha comunicação interna
    - Aceitação de Proposta
        - Inadequação da concepção
        - Falta de manutenção/controle
        - Falha comunicação interna
    - Emissão de Apólice
        - Inadequação da concepção
        - Falta de manutenção/controle
        - Falha comunicação interna

        - Outros
    - Outros
- Outros

Infraestrutura

- Lógica
    - Inadequação
    - Mau funcionamento
    - Sobrecarga
    - Outros
- Física
    - Inadequação
    - Mau funcionamento
    - Obsolescência
    - Sobrecarga
    - Outros

Eventos Externos

- Catástrofes naturais
- Atentados
- Paralisações
- Epidemias
- Outros

Buscando o desdobramento do terceiro nó, risco de pessoal, mostramos o detalhamento desse risco conforme mostrado na Figura 23 abaixo:

Figura 23: Desdobramento da folha risco de pessoal.
Fonte: O autor.

Onde ambição, insatisfação, desmotivação, zona de conforto, equívocos, negligência, omissão, distração e mão de obra não qualificada são descritos como segue:

3.13. Ambição

O risco de ambição é caracterizado pelas perdas causadas por ações negligentes de colaboradores que almejam benefício pessoal e para tal, não são medidas as consequências de suas ações.

3.14. Insatisfação

O risco de Insatisfação é definido pelas perdas decorrentes das ações negligentes de colaboradores que se sentem prejudicados pela organização de uma forma ou de outra.

3.15. Desmotivação

O risco de desmotivação é definido pelas perdas decorrentes das ações negligentes de colaboradores que não possuem clareza de motivos para suas ações.

3.16. Zona de Conforto

O risco de zona de conforto é definido pelas perdas ocasionadas por ações negligentes de colaboradores que são resistentes aos processos de mudança e/ou dinâmicos dentro da corporação.

3.17. Equívocos

O risco dado por equívocos é definido pelas perdas ocasionadas por má interpretação por parte do colaborador.

3.18. Negligência

O risco de negligência é definido pelas perdas geradas por falta de cuidado, ou seja, descuido ou desmazelo por parte do colaborador.

3.19. Omissão

O risco de omissão é definido pelas perdas onde o não cumprimento do dever por parte do colaborador é concretizado.

3.20. Distração

O risco de distração é definido pelas perdas ocasionas pela distração por parte do colaborador na execução de suas tarefas.

3.21. Mao de obra não qualificada

O risco de mão de obra não qualificada é definido pelas perdas ocasionadas por colaboradores desempenhando funções para as quais não foram qualificados, sejam por experiências anteriores e/ou novos treinamentos.

Unindo as folhas um, dois e três teremos uma visão macro da proposta de classificação de risco operacional em uma estrutura taxonômica. Essa visão pode ser verificada na figura 24.

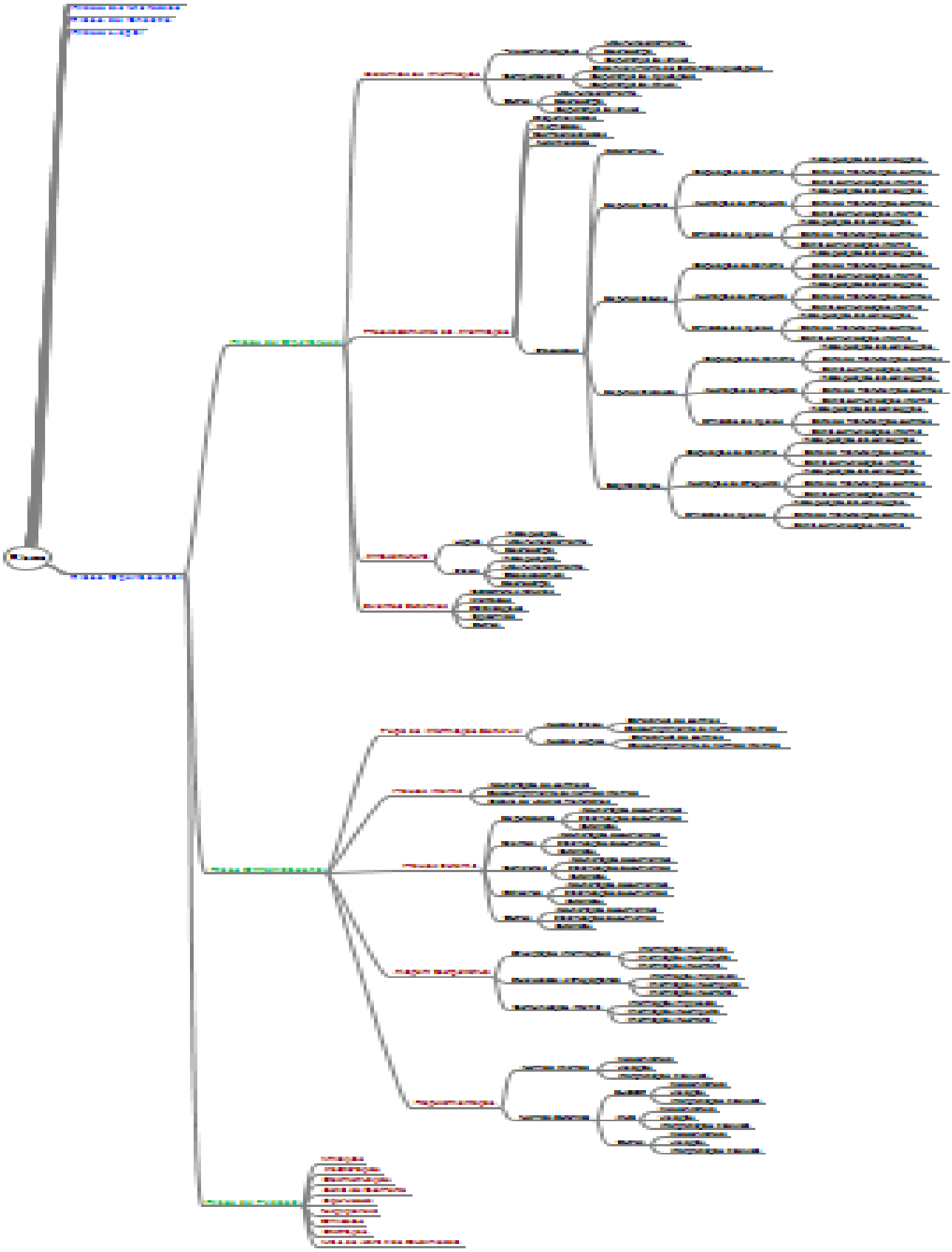


Figura 24: Macro visão classificação de risco operacional em estrutura taxonômica

Fonte: O autor.

4. Estudo de Caso

Apresentamos neste capítulo o estudo de caso referente a aderência da proposta de classificação de risco operacional e sua estrutura taxonômica para empresas do mercado segurador.

Para que o estudo de caso tenha sua confiabilidade aumentada é necessário a utilização de um protocolo onde algumas regras gerais devem ser seguidas ao se utilizar o instrumento. Sua organização está disposta conforme as seguintes seções: visão geral, procedimentos de campo, questões e relatório (YIN, 2001).

4.1. Visão Geral

Ainda segundo Yin (YIN, 2001) uma visão geral do projeto do estudo de caso deve incluir as informações prévias sobre o projeto, as questões imperativas e as leituras relevantes a essas questões. Quanto as informações prévias, cada projeto possui seu próprio contexto e perspectiva (YIN, 2001).

4.1.1. Contexto

A empresa estudada faz parte de um complexo empresarial cooperativo. O complexo tem sua origem em 1967, na cidade de Santos, com a criação da primeira cooperativa de trabalho na área de medicina do país. Na esteira de sua fundação foram, nos anos seguintes, criadas e implantadas outras unidades nos estados do Rio Grande do Sul, Minas Gerais, Rio de Janeiro, Santa Catarina, Brasília, entre outros. Nos anos 70, visando padronizar procedimentos operacionais e estimular a troca de experiências entre as cooperativas de um mesmo estado, são criadas as Federações e, em 1975, a Confederação Nacional das Cooperativas, entidade máxima do sistema cooperativo que congrega federações e cooperativas individuais de todo o país. Em 1987, existiam 60 empresas em todo o Brasil, passando a 100 cooperativas nos anos 80.

Atualmente, o Sistema conta com 377 cooperativas médicas entre Singulares, que atuam no âmbito dos municípios e oito Federações – organização de singulares em um mesmo estado. Na região Sul do País, as Federações do Paraná, Santa Catarina e Rio Grande do Sul formam a empresa do MERCOSUL. As Federações, por sua vez, reúnem-se em uma Confederação Nacional, com abrangência em 75% do território nacional, em mais de 4.125 municípios brasileiros.

A rede de assistência médica reúne 106 mil médicos cooperados, também possui 3.596 hospitais credenciados, além de pronto-atendimentos, laboratórios, ambulâncias e hospitais próprios e credenciados, para garantir qualidade na assistência médica, hospitalar e de diagnóstico complementar oferecidos. Ao todo, o sistema presta assistência para mais de 14,6 milhões de clientes e 73 mil empresas, nas mais diversas modalidades de seguro, com faturamento de R$_800 milhões aproximadamente no ano de 2010 e o Complexo Empresarial Cooperativo é composto de outras empresas, criadas para oferecer suporte ao Sistema.

Missão

Oferecer soluções em seguros, atendendo às necessidades das cooperativas e do mercado em geral.

Visão

Ser reconhecida como uma empresa do sistema cooperativo com excelência em seguros.

Valores

Valorização do Colaborador:

Criar e proporcionar oportunidades e meios de desenvolvimento e crescimento, reconhecendo a importância das qualidades, potencialidades, méritos pessoais e profissionais do ser humano.

Compromisso com o Cliente

Conhecer bem as necessidades dos clientes e buscar entregar-lhes o melhor.

Melhoria Contínua

Buscar constantemente o aperfeiçoamento dos sistemas de gestão, tecnologia e comunicação, aprimorando seus processos, produtos e relacionamento com todos os públicos estratégicos.

Fazer a Diferença

Atuar na sociedade por meio de relacionamentos e parcerias que busquem o bem comum, fazendo escolhas inovadoras, com novas e melhores formas de pensar e agir.

4.1.1.1. Objetivo

O objetivo do estudo de caso é verificar a aderência da proposta de classificação de risco operacional e sua estrutura taxonômica para empresas do mercado segurador.

4.1.1.2. Envolvidos

No estudo de caso estão envolvidos um superintendente executivo com doze anos de empresa, um gerente de gestão de riscos com oito anos no cargo, um consultor interno da área de gestão de riscos, há quinze anos na empresa, dois analistas juniores da área de gestão de riscos: seis anos e um ano respectivamente e um consultor externo.

4.1.2. Questões que estão sendo estudadas

O estudo de caso tem como objetivo analisar a hipótese da usabilidade e padronização para riscos operacionais através da aderência da proposta de classificação de risco operacional e sua estrutura taxonômica para empresas do mercado segurador. O objetivo de validação da usabilidade e aderência do modelo proposto será alcançado através da identificação dos riscos atuais e mapeados pela unidade responsável e confrontá-los com a proposta de classificação de risco operacional e sua estrutura taxonômica. A verificação dos riscos existentes deverá ser realizada através de dicionário de risco ou equivalente.

Assim, podemos identificar se há divergência entre os riscos atuais levantados pela área responsável e a proposta de classificação de risco operacional e sua estrutura taxonômica. A amostra selecionada é composta por todos os riscos classificados como do tipo operacional e que atualmente fazem parte da carteira da área de gestão de riscos.

4.1.3. Leituras relevantes sobre as questões estudadas

É de extrema relevância a leitura dos capítulos 2, especialmente os itens 2.1 que nos mostra uma visão geral do mercado segurador brasileiro, 2.2 que trata de risco e suas divisões, 2.3 onde taxonomia é abordada, 2.4 que detalha sobre segurança da informação e por fim, o capítulo 3 onde a proposta de classificação de risco operacional e sua estrutura taxonômica para empresas do mercado segurador são detalhadas.

4.2. Procedimentos de campo

Ainda segundo Yin (YIN, 2001), procedimentos de campo são de extrema importância e os dados devem ser coletados de pessoas e de entidades reais e não de laboratórios de forma que o ambiente onde a coleta foi realizada não sofra interferência por parte do pesquisador.

Não houve dificuldades para que o pesquisador tivesse acesso aos entrevistados visto que o mesmo faz parte do mercado segurador. Como ferramental, questionários elaborados pelo pesquisador são utilizados para a coleta de dados. Tais questionários são respondidos e preenchidos por diferentes pessoas integrantes da área de gestão de riscos e também com diferentes níveis hierárquicos.

4.3. Questões

O conjunto de questões substantivas que refletem a investigação real é ponto central do protocolo utilizado. As questões utilizadas pelo pesquisador devem possuir duas características: perguntas feitas ao pesquisador, e não ao respondente e também cada questão deve vir acompanhada por uma lista de prováveis evidências como, por exemplo, a identificação do respondente. Essas duas características diferem as questões de um estudo de caso e um levantamento (YIN, 2001). Todas as questões substantivas que refletem a investigação encontram-se no apêndice A. As questões entregues aos entrevistados, nível um, encontram-se no APÊNDICE A.

4.4. Relatório

O relatório será apresentado como narrativa simples para descrever e analisar o estudo de caso (YIN, 2001). O propósito de validar a proposta de classificação para riscos operacionais e sua disposição em uma estrutura taxonômica para empresas do mercado segurador brasileiro sob a visão da segurança da informação foi realizado através de aplicação de questionário para área específica de gestão de risco segundo critérios já discutidos através do protocolo do estudo de caso. Ainda, objetivando a proteção do caso real e de seus participantes o mais comum é o anonimato (YIN, 2001). Não somente a identidade da empresa estudada e os nomes dos participantes foram mantidos em sigilo, mas também os dados relacionados ao estudo de caso.

Buscando a confiabilidade do estudo de caso, todas as evidências para o estudo provêm de registros em arquivos, entrevistas e observação direta. Cada evidência possui pontos fortes e fracos, de acordo com Yin (YIN, 2001) esses pontos são demonstrados no Quadro 1.

Quadro 1: Pontos fortes e fracos das fontes de evidências utilizadas.

Fonte da evidência	Pontos fortes	Pontos fracos
Registro em arquivos	• Estáveis: os registros podem ser revisados várias vezes; • Discretos: não foram criados como resultado do estudo de caso; • Exatos: contém nomes, referências e detalhes exatos de um evento; • Ampla cobertura: longo espaço de tempo, muitos eventos e muitos ambientes distintos; • Preciso e quantitativo.	• Capacidade de recuperação pode ser baixa; • Seletividade tendenciosa; • Relato de visões tendenciosas; • Acesso pode ser deliberadamente negado.
Entrevistas	• Direcionadas: enfocam diretamente o tópico do estudo de caso; • Perceptivas: fornecem inferências causais percebidas.	• Visão tendenciosa devido a questões mal elaboradas; • Respostas tendenciosas; • Ocorrem imprecisões devido à memória fraca do entrevistado; • Reflexibilidade – o entrevistado dá ao entrevistador o que ele quer ouvir.
Observação direta	• Realidade – tratam de acontecimentos em tempo real; • Contextuais – tratam do contexto do evento.	• Consomem muito tempo; • Seletividade; • Reflexibilidade; • Custo – horas necessárias pelos observadores humanos;

Fonte: (YIN, 2001)

O registro em arquivos, como por exemplo, o dicionário de risco utilizado antes da apresentação do modelo proposto, é fundamental para validar os conceitos contidos no modelo proposto bem como sua estrutura taxonômica. As entrevistas foram do tipo focal, onde o respondente é entrevistado por um curto período de tempo. Essas entrevistas são espontâneas e assumem o caráter de uma conversa informal (YIN, 2001). Por fim, na observação direta, o pesquisador apesar de não inferir diretamente na operação do dia-a-dia da área de gestão de riscos, mas pôde de maneira informal realizar observações diretas ao longo da visita de campo.

Anteriormente a aplicação do questionário, demonstrado no APÊNDICE A, foi realizado algumas verificações quanto à pré-existência de metodologia aplicada à gestão de riscos e consequentemente a classificação de riscos operacionais.

A área de gestão de riscos da empresa onde foi realizado o estudo de caso já utilizava metodologia de mercado para as práticas de gestão. No que tange a classificação de risco, a empresa objeto de estudo, possui dicionário de risco onde todos os riscos estavam classificados em nove grandes categorias e vinte e sete subcategorias. Quanto ao risco operacional, este estava subdividido em apenas dez subgrupos conforme mostrado na Figura 24 abaixo:

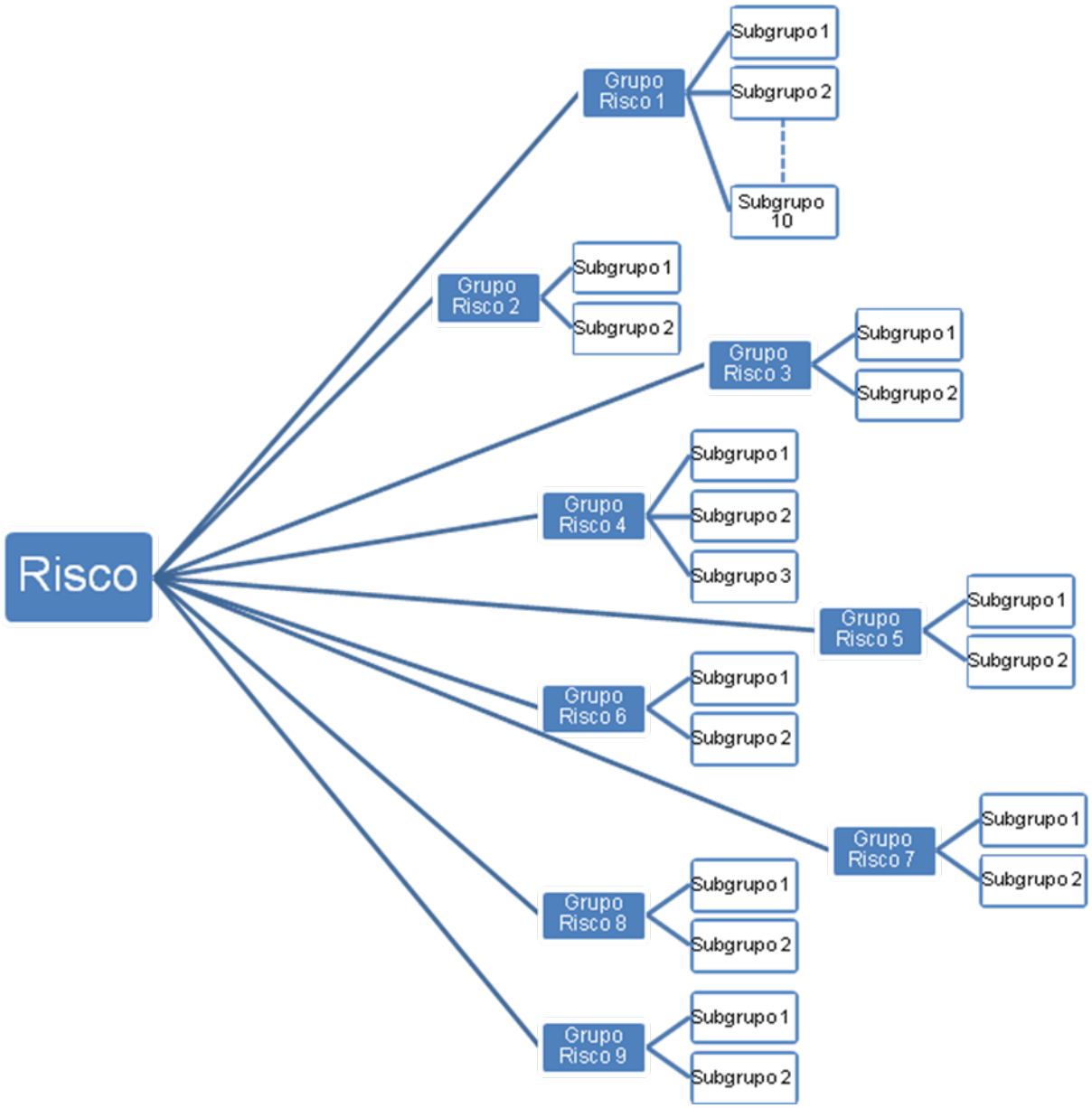


Figura 25: Classificação de risco do objeto de estudo

Fonte: O autor.

Com base no questionário, apresentado no APÊNDICE A, foi verificado inicialmente a aderência quanto aos termos utilizados bem como o conceito de cada um deles. A concordância foi verdadeira em sua totalidade havendo apenas pequenas divergências para um ou outro item. Na sequência, foi verificado quanto a aderência do modelo proposto confrontando com o atual dicionário de riscos da empresa e sua aderência foi integral. Para que fosse possível a aderência integral, houve a necessidade de remanejamento de algumas categorias e consequentemente de alguns subgrupos de forma que todos se adequassem ao modelo proposto. Com o modelo proposto, a disposição dos riscos operacionais tornou-se mais clara e em conformidade com melhores práticas de mercado.

Quanto à usabilidade do modelo proposto para classificação de riscos operacionais e sua estrutura taxonômica para empresas do mercado segurador brasileiro, foi verificado que sua usabilidade é integral com as operações da área de gestão de riscos do objeto estudado. Todos os resultados foram extraídos das evidências segundo o protocolo do estudo de caso incluindo os resultados das respostas do questionário aplicado. Esses resultados estão dispostos conforme mostrado na Figura 26.

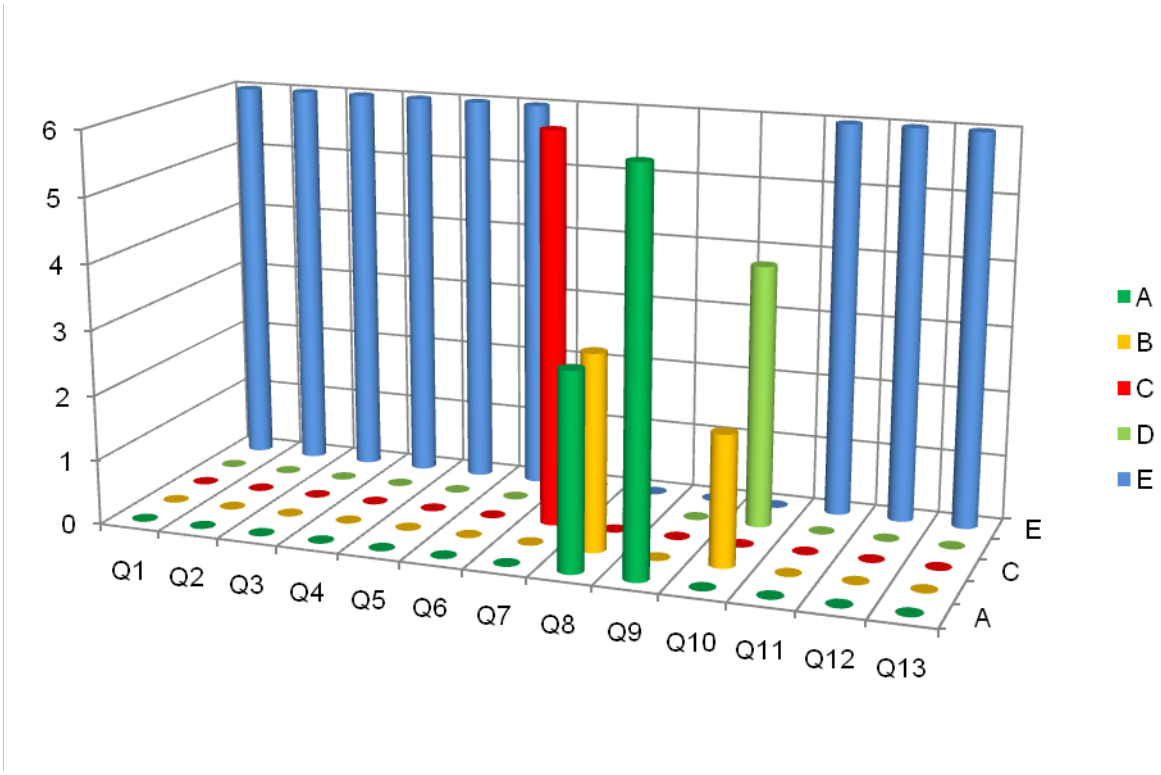


Figura 26: Resultado questionário apêndice A.

Fonte: O autor.

Ainda na Figura 26, todas as treze questões do questionário do apêndice A estão dispostas de Q1 a Q13. Cada questão possui cinco alternativas, que na Figura 26 estão dispostas de A a E. Por fim, para que fosse possível a quantificação para cada pergunta, a representação de 0 a 6 foi utilizada na mesma figura.

5. Conclusões

O mercado segurador brasileiro tem se mostrado ativo e crescente ao longo dos últimos anos. As expectativas do setor são as melhores possíveis e com elas crescem também as preocupações em relação a riscos e consequentemente à informação, ativo intangível de alto valor para as organizações. No intuito de contribuir para o melhor gerenciamento de riscos de uma empresa, mapear, classificar os riscos inerentes ao negócio é de extrema necessidade e importância e somente a partir da posse dessas informações é possível organizar as ações de mitigação dos mesmos.

Apesar dos órgãos normativos, que buscam o controle do mercado segurador brasileiro, através de regulamentações específicas para o tratamento de riscos para o setor, há uma deficiência em seu detalhamento dificultando a implementação de quaisquer que sejam os controles adotados pelas empresas. O fato é que mais e mais essas regulamentações têm exigido das corporações maior rigor no tratamento da informação de forma geral, exigindo assim que a segurança da informação seja aplicada com maior seriedade e voltada ao negócio. O mercado segurador brasileiro necessita de uma padronização quanto ao entendimento conceitual e classificação de seus riscos.

O objetivo principal desta pesquisa, propor a classificação para riscos operacionais e sua disposição em uma estrutura taxonômica para empresas do mercado segurador brasileiro sob a visão da Segurança da Informação, foi atendido conforme delineado através dos capítulos fundamentação teórica, capítulo 2, modelo proposto, capítulo 3 e estudo de caso no capítulo 4.

O modelo proposto de classificação para riscos operacionais foi fundamentado de acordo com o estudo teórico e empírico. Parte da contribuição foi dada, apesar de ser aplicado em outra área, pelo *Software Engineering Institute - SEI* da *Carnegie Mellon University* que através de questionários taxonômicos pôde mapear riscos associados ao desenvolvimento de software. Como resultado uma distribuição dos tais riscos em três principais níveis de riscos. O mesmo princípio foi adotado para a composição do modelo proposto onde foram assumidos conceitos baseados na legislação atual do setor unindo-os a níveis empíricos e com maior detalhamento. O

resultado foi uma classificação para riscos operacionais onde o mesmo é subdividido em três principais categorias chamadas de nós: risco organizacional, risco de operações e risco de pessoal, onde cada nó possui sua própria definição. Cada nó é então subdividido em mais um nível de detalhamento, também chamados de nós, perfazendo um total de dezoito deles. Posteriormente cada nó, por sua vez, possui até quatro subníveis de detalhamento totalizando cento e trinta e três possíveis riscos dentro da estrutura taxonômica.

Os objetivos específicos também foram alcançados conforme disposto no capítulo 4, estudo de caso onde, através de questionário foi evidenciada a contribuição para o detalhamento da classificação de riscos para o mercado segurador brasileiro. Ainda através do questionário, foi percebida uma contribuição para a conceituação de estruturas taxonômicas conforme detalhado no capítulo 3. O questionário ainda nos mostra a total aderência do modelo proposto no que tange a classificação de riscos operacionais para empresas do mercado segurador brasileiro.

Finalmente, com a conclusão desta pesquisa, corroborou-se a hipótese levantada desde o início do estudo, confirmando que a padronização da classificação para riscos operacionais, dispostos em uma estrutura taxonômica, para empresas do mercado segurador brasileiro é possível e com excelente aderência conforme evidenciado através do estudo de caso.

6. Trabalhos futuros

Em função da amplitude e da relevância do tema, sugere-se para as pesquisas futuras a validação do modelo de classificação de risco operacional para o mercado segurador brasileiro em um número maior de empresas desse seguimento, através de aplicação de questionário, buscando também sua aderência e usabilidade junto à empresa estudada.

Sugere-se também que, ainda em continuação a esta pesquisa, ferramentas específicas para a representação taxonômica seja elencadas, devidamente validadas junto ao mercado segurador.

Para finalizar, propostas de classificação para riscos operacionais e sua disposição em uma estrutura taxonômica, devem-se expandir para outras áreas e mercados.

7. REFERÊNCIAS BIBLIOGRÁFICAS

(ISC)2. **International Information Systems Security Certification Consortium Inc.** Disponivel em: <http://www.isc2.org>. Acesso em: 5 Maio 2010.

27002:2005, A. N. I. **ABNT NBR ISO/IEC 27002:** 2005. [S.l.]: [s.n.], 2005.

ABBOTT, R. P. et al. **Security Analysis and Enhancements of Computer Operating Systems**. National Bureau of Standards. Washington, DC. 1976.

ABNT, I. **ABNT ISO/IEC 73:** 2009 Gestão de Risco - Vocabulário. Rio de Janeiro: [s.n.], 2009.

ALBERTIN, A. L. **Benefício do Uso de Tecnologia de Informação no Desempenho Empresarial**. Fundação Getúlio Vargas. São Paulo. 2005.

ANDRADE, A.; ROSSETTI, J. P. **Governança Corporativa:** Fundamentos, Desenvolvimento e Tendências. [S.l.]: Atlas, 2004.

BAILEY, K. D. **Typologies and Taxonomies:** An introduction to Classification Techniques. [S.l.]: SAGE Publications, 1994.

BERNSTEIN, P. L. **Against the Gods - The Remarkable Story of Risk**. [S.l.]: John Wiley & Sons Inc, 1998.

BLACKBURN, B. Taxonomy Design Types. **AIIM e-Doc**, Maryland, v. 20, n. 3, May/June 2006.

BRASIL, B. C. D. Busca de Normativos. **Banco Central do Brasil**, 2010. Disponivel em: <https://www3.bcb.gov.br/normativo/detalharNormativo.do?method=detalharNormativo&N=106196825>. Acesso em: 05 Agosto 2010.

CAMPOS, M. L. D. A. Modelização de domínios de conhecimento: uma investigação de princípios fundamentais. **Ci. Inf.**, Brasília, Abril 2004. 22-32.

CARR, M. J. et al. **Taxonomy-Based Risk Identification**. Carnegie Mellon University. Pittsburgh, PA. 1993.

CARVALHO, F. A. Os efeitos da adoção dos conceitos e das práticas de governança corporativa na transparência das informações evidenciadas por empresas brasileiras do setor de papel e celulose. **IBGC - Instituto Brasileiro de Governança Corporativa**, 2004.

CNSEG. **Informe Anual Balanço Social 2009**. FENASEG. Rio de Janeiro. 2010.

CONWAY, S.; SLIGAR, C. Unlocking Knowledge Assets. **Microsoft Learning**, 2003. Disponivel em: <http://www.microsoft.com/mspress/books/sampchap/5516.aspx>. Acesso em: 03 Outubro 2010.

CORPORATIVA, I. B. G. **Código das Melhores de Governança Corporativa**. IBGC. [S.l.]. 2010.

COSO, T. C. O. S. O. O. T. T. C.-. **Gerenciamento de Riscos Corporativos - Estrutura Integrada**. New York: American Institute of CPAs, 2007.

DHILLON, G.; BACKHOUSE, J. Information system security management in the new millennium. **Communications of the ACM**, 2000.

DRUCKER, P. **Desafios gerenciais para o século XXI.** São Paulo: Thomson Pioneira, 1999.

DUARTE JR., A. M. Risco: definições, tipos, medição e recomendações para seu gerenciamento. **Resenha BM&F**, 01 nov. 1996.

DUARTE JR., A. M. A Importância do Gerenciamento de Riscos Corporativos. **Risk Tech**, 2010. Disponivel em: <http://www.risktech.com.br/PDFs/RISCORPO.pdf>. Acesso em: 01 Outubro 2010.

DUTRA, J.; BUSCH, J. Taxonomy Strategies. **Enabling Knowledge Discovery:** Taxonomy Development for NASA, 2003. Disponivel em: <http://www.xml.gov/documents/completed/nasa/index.html>. Acesso em: 04 Outubro 2010.

FENASEG. Sistema Nacional de Seguros Privados. **Estrutura**, 2010. Disponivel em: <http://www.fenaseg.org.br/>. Acesso em: 05 fev. 2011.

FENASEG. História do Seguro no Brasil. **História do Seguro**, 2011. Disponivel em: <http://www.fenaseg.org.br/>. Acesso em: 05 fev. 2011.

FERREIRA, A. B. D. H. Aurélio Século XXI. In: _____ **Novo Aurélio Século XXI - O Dicionário da Língua Portuguesa**. 3a. ed. São Paulo: Editora Nova Fronteira, 1999. p. 1829.

FERREIRA, A. B. D. H. Aurélio Século XXI. In: _____ **Novo Aurélio Século XXI - O Dicionário da Língua Portuguesa**. 3a. ed. São Paulo: Editora Nova Fronteira, 1999. p. 1830.

FERREIRA, R. C. **Proposta de um Modelo para Avaliação de Risco Operacional em Empresa não Financeiras: Estudo de Caso de uma Empresa de Telecomunições no Brasil**. Faculdade de Economia e Finanças IBMEC. Rio de Janeiro. 2006.

FORUM, I. S. M. **An Introductory Overview of ITIL v3**. Office of Government Commerce (OGC). [S.l.]. 2007.

GALLAGHER, B. P. et al. **A Taxonomy of Operational Risks**. Carnegie Mellon University. Pittsburgh, PA. 2005.

GIL, A. C. **Como Elaborar Projetos de Pesquisa**. 4a. ed. São Paulo: Atlas, 2002.

GLOBAL, S. AS/NZS ISO 31000:2009 Risk management - Principles and guidelines. **SAI Global InfoStore**, 2011. Disponivel em: <http://infostore.saiglobal.com/store/Details.aspx?ProductID=1378670>. Acesso em: 23 fev. 2011.

GREMBERGER, W. V. **Strategies for Information Technology Governance**. [S.l.]: Idea Group Publishing, 2004.

GRÜN, R. Atores e ações na construção da governança corporativa brasileira. **Revista Brasileira de Ciências Sociais**, 2003. Disponivel em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-69092003000200008>. Acesso em: 14 Dezembro 2009.

HARRIS, S. **CISSP All in One Exam Guide**. 5a. ed. [S.l.]: McGraw-Hill Osborne Media, 2010.

IEEE. **Standard Glossary of Software Engineering Terminology**. IEEE. New York. 1990.

INSTITUTE, I. T. G. CobiT 4.1. **CobiT 4.1**, 2007.

ISO/IEC, A. **ABNT ISO/IEC 27005 Tecnologia da Informação - Técnicas de Segurança - Gestão de Riscos de Segurança da Informação**. Rio de Janeiro: [s.n.], 2008.

ISO/IEC, A. **ABNT ISO/IEC 31000:** 2009 Gestão de Riscos - Princípios e Diretrizes. Rio de Janeiro: [s.n.], 2009.

ITGI. **Board Briefing on IT Governance**. IT Governance Institute. [S.l.]. 2006.

JR., S. D.; GALIZA, F. **Indústria Seguradora do Brasil: Visão Executiva da Situação Atual e Perspectivas para 2015**. Accenture. [S.l.]. 2010.

KAPLAN, R. S.; NORTON, D. P. **Strategy Maps - Converting Intangible Assets Into Tangible Outcomes**. [S.l.]: Harvard Business Publishing Corporation, 2004.

KRAFZIG, D.; BANKE, K.; SLAMA, D. **Enterprise SOA:** Service-Oriented Architecture Best Practices. [S.l.]: Prentice Hall, 2004.

LETHBRIDGE, E. Governaça Corporativa. **BNDES**, 1997. Disponivel em: <http://www.bndes.gov.br/SiteBNDES/export/sites/default/bndes_pt/Galerias/Arquivos/conhecimento/revista/rev809.pdf>. Acesso em: 16 dez. 2009.

LIEBER, R. R.; LIEBER, N. S. R. O conceito de Risco: Janus reinventado. **Minayo MCS & Miranda AC Saúde e ambiente: Estreitando nós**, Rio de Janeiro, 2002. 69-112.

LOPES, C. O que é Governança Corporativa? **iMasters**, 2006. Disponivel em: <http://imasters.uol.com.br/artigo/3941/governanca/o_que_e_governanca_corporativa/>. Acesso em: 16 Janeiro 2010.

LUFTMAN, J. Assessing Business-IT Alignment Maturity. **Communications of Association for Information Systems**, 2000.

LUFTMAN, J. N.; PAPP, R.; BRIER, T. Eablers and Inhibitors of Business-IT Alignment. **Communications of the Association for Information Systems**, 1999.

MILLER, D. Relating Porter's Business Strategies to environment and structure: analysis and performance. **Academy of Management Journal**, 1998. 208-308.

OB-007 COMMITTEE. **Risk management AS/NZS 4326:** 2004. 3a. ed. Sidney: Standards Australia/Standards New Zealand, 2004.

OECD. Principles for Corporate Governance. **OECD**, 2010. Disponivel em: <http://www.oecd.org/publications/0,2743,en_2649_201185_1_1_1_1_1,00.html>. Acesso em: 05 Fevereiro 2010.

PARKER, D. B. **Toward a New Framework for Information Security - The Computer Security Handbook**. 4a. ed. [S.l.]: [s.n.], 2002.

PFLEEGER, C. P. E. P. **Security in Computing**. 4a. ed. [S.l.]: Prentice Hall, 2006.

SALOMON, D. **Foundation of Computer Security**. [S.l.]: Springer-Verlag London Limited, 2006.

SPINK, M. J. Trópicos do discurso sobre risco: risco-aventura como metáfora na modernidade tardia. **Caderno Saúde Pública**, Rio de Janeiro, Nov-Dez 2001. 1277-1311.

STREIT, R. E.; MAÇADA, A. C. G.; BORENSTEIN, D. Tecnologia da Informação na Governança do Sistema Financeiro Nacional (SFN). **Congresso Anual de Tecnologia de Informação**, São Paulo, 2004.

SUSEP. Circular 249 SUSEP. **Superintendência de Seguros Privados - SUSEP**, 2004. Disponivel em: <http://www.susep.gov.br/textos/circ249.htm>. Acesso em: 10 fev. 2011.

TEO, T. S. H.; KING, W. R. Integration Between Business Planning and Information systems Planning - An Evolutionary Contingency Perspective. **Journal of Management Information Systems**, 1997. 185-214.

TERRA, J. C. C. E. A. Taxonomia: Elemento Fundamental para Gestão do Conhecimento. **Terra Forum**, 02 Outubro 2010.

THO, I. Managing the Risks of IT Outsourcing. **Computer Weekly Professional Series**, Oxford, 2005.

UNIVERSITY, P. WordNet Search. **WordNet Search**, 2010. Disponivel em: <http://wordnetweb.princeton.edu>. Acesso em: 23 Junho 2010.

WEILL, P.; ROSS, J. W. **IT Governance:** How Top Performers Manage IT Decision Rights for Superior Results. 1. ed. [S.l.]: [s.n.], 2004.

YIN, R. K. **Estudo de Caso:** Planejamento e Métodos. 2a. ed. Porto Alegre: Bookman, 2001.

APÊNDICE A. Questões do protocolo entregues aos entrevistados.

1) Com a publicação da circular SUSEP № 249, fica estabelecido a necessidade de implantação de controles internos. Com relação a essa circular como você classificaria sua adoção?
   A. A empresa não está em conformidade com a circular SUSEP № 249.
   B. A área de gestão de riscos está parcialmente em conformidade com a circular SUSEP № 249.
   C. A área de gestão de riscos está em conformidade com a circular SUSEP № 249.
   D. A área empresa está parcialmente em conformidade com a circular SUSEP № 249.
   E. A área empresa está em conformidade com a circular SUSEP № 249.

2) A gestão de risco é um dos controles exigidos pela circular SUSEP № 249. Como você classificaria a existência de uma área específica para gestão de riscos dentro da empresa?
   A. A área de gestão de riscos é inexistente e não há controle dos riscos associados às atividades da empresa.
   B. A área de gestão de riscos é inexistente e há controle parcial dos riscos associados às atividades da empresa.
   C. A área de gestão de riscos é inexistente e há controle integral dos riscos associados às atividades da empresa.
   D. A área de gestão de riscos existe e há controle parcial dos riscos associados às atividades da empresa.
   E. A área de gestão de riscos existe e há controle integral dos riscos associados às atividades da empresa.

3) Ainda com relação a circular SUSEP № 249, como você classificaria a implementação de controles internos junto à empresa?
   A. A implementação de controles internos é inexistente.
   B. A implementação de controles internos foi realizada de forma parcial na área de gestão de riscos.

C. A implementação de controles internos foi realizada de forma integral somente na área de gestão de riscos.
D. A implementação de controles internos foi realizada de forma parcial em toda a empresa.
E. A implementação de controles internos foi realizada de forma integral em toda a empresa.

4) As atividades de gestão de risco, seja através de área específica ou não, devem ser sistematicamente verificadas. Como você classificaria quanto à utilização de metodologia de mercado, no controle dessa verificação?
A. Não há adoção de metodologia de mercado para controle/verificação das atividades de gestão de risco.
B. Não há adoção de metodologia de mercado, mas há controle/verificação parcial das atividades de gestão de risco.
C. Não há adoção de metodologia de mercado, mas há controle/verificação integral das atividades de gestão de risco.
D. Há adoção de metodologia de mercado e há controle/verificação parcial das atividades de gestão de risco.
E. Há adoção de metodologia de mercado e há controle/verificação integral das atividades de gestão de risco.

5) Ainda para atividades de gestão de risco, como você classificaria quanto à utilização de ferramental para apoiar tais atividades?
A. Não há adoção de ferramental de mercado para apoiar as atividades de gestão de risco.
B. Há adoção de ferramental livre (*opensource*), sem a contratação de suporte, para apoiar as atividades de gestão de risco.
C. Há adoção de ferramental livre (*opensource*), com a contratação de suporte, para apoiar as atividades de gestão de risco.
D. Há adoção de ferramental de mercado, sem a contratação de suporte, para apoiar as atividades de gestão de risco.
E. Há adoção de ferramental de mercado, com a contratação de suporte, para apoiar as atividades de gestão de risco.

6) Com relação à classificação de riscos, como você classificaria sua existência?
   A. A classificação de riscos para a área gestão de riscos é inexistente.
   B. A classificação de riscos para a empresa é inexistente.
   C. A classificação de riscos é existente e somente utilizada pela área de gestão de riscos.
   D. A classificação de riscos é existente e interna.
   E. A classificação de riscos é existente e baseada em melhores práticas de mercado.

7) Com relação a dicionário de riscos, como você classificaria sua existência?
   A. O dicionário de riscos é inexistente.
   B. O dicionário de riscos é existente, de uso parcial e de responsabilidade da área de gestão de riscos.
   C. O dicionário de riscos é existente, de uso integral e de responsabilidade da área de gestão de riscos.
   D. O dicionário de riscos é existente, de uso parcial e não é responsabilidade da área de gestão de riscos.
   E. O dicionário de riscos é existente, de uso integral e não é responsabilidade da área de gestão de riscos.

8) Sendo a taxonomia uma ciência de identificação que pode ser utilizada para o desígnio de conjuntos de termos representativos de uma determinada área, estruturados de forma hierárquica, como você classificaria sua existência para apoiar a gestão de riscos?
   A. Não há taxonomia existente para apoiar a gestão de riscos.
   B. Há taxonomia representativa, parcial, para apoiar a gestão de riscos e de responsabilidade da área de gestão de riscos.
   C. Há taxonomia representativa, integral, para apoiar a gestão de riscos e de responsabilidade da área de gestão de riscos.
   D. Há taxonomia representativa, parcial, para apoiar a gestão de riscos e não de responsabilidade da área de gestão de riscos.
   E. Há taxonomia representativa, integral, para apoiar a gestão de riscos e não de responsabilidade da área de gestão de riscos.

9) Em caso afirmativo para a existência de uma taxonomia para apoiar a gestão de riscos, como você classificaria a utilização de ferramental para tal?
   A. Não há adoção de ferramental de mercado para apoiar a utilização de taxonomia.
   B. Há adoção de ferramental livre (*opensource*), sem a contratação de suporte, para apoiar a utilização de taxonomia.
   C. Há adoção de ferramental livre (*opensource*), com a contratação de suporte, para apoiar a utilização de taxonomia.
   D. Há adoção de ferramental de mercado, sem a contratação de suporte, para apoiar a utilização de taxonomia.
   E. Há adoção de ferramental de mercado, com a contratação de suporte, para apoiar a utilização de taxonomia.

10) Considerando que Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio, como você classificaria a existência de Segurança da Informação?
   A. Não há Segurança da Informação dentro da empresa.
   B. Há Segurança da Informação internamente implantada de forma parcial na empresa.
   C. Há Segurança da informação internamente implantada de forma integral na empresa.
   D. Há Segurança da informação externamente implantada de forma parcial na empresa.
   E. Há Segurança da Informação externamente implantada de forma integral na empresa.

11) Após o entendimento da proposta de classificação de riscos operacionais, como você classificaria sua aderência à estrutura de riscos existentes da empresa?
   A. Não há aderência alguma.
   B. Há alguma aderência.
   C. Há aderência, mas necessita de pequenas adequações.
   D. Há aderência, mas necessita de grandes adequações.
   E. Há aderência em sua totalidade.

12) Com relação a disposição da classificação de riscos operacionais em uma estrutura taxonômica, como você classificaria sua usabilidade?
   A. Nenhuma usabilidade.
   B. Alguma, menor que 25%, usabilidade.
   C. Pequena, menor que 50%, usabilidade.
   D. Sua usabilidade é parcial.
   E. Sua usabilidade é integral.

13) Tomando como base a proposta de classificação de risco operacional e sua representação em uma estrutura taxonômica, como você classificaria sua adoção para representar a atual carteira de riscos operacionais da empresa?
   A. Nenhuma adoção.
   B. Alguma, menor que 25%, de adoção.
   C. Pequena, menor que 50% de adoção.
   D. Adoção parcial.
   E. Adoção integral.